

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL.,

Plaintiffs,

vs.

CIVIL ACTION FILE
NO. 1:17-CV-2989-AT

BRAD RAFFENSPERGER, ET AL.,

Defendants.

VIDEOTAPED ZOOM DEPOSITION OF
JAMES OLIVER

January 17, 2022
8:09 A.M.

Lee Ann Barnes, CCR-1852B, RPR, CRR, CRC

APPEARANCES OF COUNSEL
(All appearances via Zoom)

On behalf of the Plaintiffs:

DAVID D. CROSS, ESQ.
MARY G. KAISER, ESQ.
MORRISON & FOERSTER LLP
2100 L Street, NW
Suite 900
Washington, DC 20037
202.887.8795
dcross@mofo.com
mkaiser@mofo.com

- and -

HALSEY G. KNAPP, JR., ESQ.
KREVOLIN HORST
One Atlantic Center
1201 W. Peachtree Street, NW
Suite 3250
Atlanta, Georgia 30309
404.888.9700
hknapp@khlawfirm.com

On behalf of Secretary of State and the State
Election Board:

DIANE F. LaROSS, ESQ.
BRYAN P. TYSON, ESQ.
1600 Parkwood Circle, SE
Suite 200
Atlanta, Georgia 30339
678.336.7249
dlaross@taylorenghish.com
btyson@taylorenghish.com

APPEARANCES OF COUNSEL

On behalf of Defendants Fulton County Voter
Registration and Elections:

DAVID LOWMAN, ESQ.
OFFICE OF THE FULTON COUNTY ATTORNEY
141 Pryor Street, SW
Suite 4038
Atlanta, Georgia 30303
david.lowman@fultoncountyga.gov

Also Present:

Jonathan Miller, Videographer
Grace Huff, Concierge Tech

INDEX OF EXAMINATION

WITNESS: JAMES OLIVER

EXAMINATION

PAGE

By Mr. Cross

8

INDEX TO EXHIBITS

Plaintiffs'			
Exhibit	Description	Page	
Exhibit 1	Org Chart, Bates No. FORTALICE000254	17	
Exhibit 2	LinkedIn Profile of James Oliver, no Bates numbers	27	
Exhibit 3	Fortalice Task Order dated 3/11/21, Bates Nos. FORTALICE000001 through -2	60	
Exhibit 4	Email Chain dated October 2018, Bates Nos. FORTALICE000995 through -998	66	
Exhibit 5	Email Chain dated August 2016, Bates Nos. FORTALICE000002952 through -2953	77	
Exhibit 6	2020 Rule 590-8.3 Attestation, Bates Nos. STATE-DEFENDANTS-00182173 through -182175	81	
Exhibit 7	Email Chain dated April 2019, Bates No. STATE-DEFENDANTS-00104972	90	
Exhibit 8	Email Chain dated October 2019, Bates Nos. STATE-DEFENDANTS-00112738 through -112740	98	
Exhibit 9	Email Chain dated July 2019, Bates Nos. STATE-DEFENDANTS-00113155 through -113156	102	
Exhibit 10	Email Chain dated April 2019, Bates Nos. STATE-DEFENDANTS-00126614 through -126616	112	

INDEX TO EXHIBITS

Plaintiffs'

Exhibit

Description

Page

Exhibit 11 Email dated 4/24/19 120
 from James Oliver to Clark
 Rainer, Bates No.
 STATE-DEFENDANTS-00146337

Exhibit 12 Email Chain dated April 129
 2019, Bates Nos.
 STATE-DEFENDANTS-00146363
 through -146371

(Original exhibits are attached to the
original transcript.)

Deposition of JAMES OLIVER

January 17, 2022

(Reporter disclosure made pursuant to
Article 8.B of the Rules and Regulations of the
Board of Court Reporting of the Judicial
Council of Georgia.)

VIDEOGRAPHER: We are on the record
January 17, 2022, at approximately 8:09 a.m.
Eastern time. This will be the videotaped
deposition of James Oliver.

Would counsel please identify themselves
and who they represent for the record.

MR. CROSS: This is David Cross of
Morrison & Foerster on behalf of the Curling
plaintiffs. And with me is my colleague, Mary
Kaiser, and Halsey Knapp.

MS. LaROSS: This is Diane LaRoss and I
represent the State defendants.

MR. TYSON: Bryan Tyson. I also represent
the State defendants. Good morning.

MR. LOWMAN: David Lowman and I represent
the Fulton County defendants.

VIDEOGRAPHER: Thank you, Counsel.

Would the court reporter please swear in

1 the witness.

2 JAMES OLIVER, having been first duly sworn, was
3 examined and testified as follows:

4 EXAMINATION

5 BY-MR. CROSS:

6 Q. Good morning, Mr. Oliver.

7 A. Good morning.

8 Q. Sorry to impose on you on a holiday.

9 Unfortunately, the timing was not of our making.

10 Have you been deposed before?

11 A. No.

12 Q. So just briefly, do you have some
13 familiarity with the way the process works? Has
14 anybody walked you through this?

15 A. State -- State counsel kind of like walked
16 me through the process, yes.

17 Q. Okay. Did you meet with counsel for the
18 State before the deposition today?

19 A. Virtually, yes.

20 Q. And how many times did you meet with them?

21 A. As far as meeting, just once. Spoke with
22 them a couple times as far as, like, telephonically.

23 Q. And about how many times did you speak
24 with them either by telephone or virtual or in
25 person?

1 A. Maybe a combination of maybe about three.

2 Q. And about how much -- how much time did
3 that take?

4 A. Encompassing everything, maybe a couple
5 hours. I'd say about three hours. Three, three and
6 a half hours, something like that --

7 Q. Okay.

8 A. -- overall, not continuously.

9 Q. Understood.

10 When was that?

11 A. Last week, Friday. Today's Monday. Last
12 week, Friday, and a couple of -- couple of times
13 telephonically prior to -- prior to -- and, I'm
14 sorry, that was Thursday. Spoke with them
15 Thursday -- last time I spoke with them was on
16 Friday, but the actual brief was on Thursday, and I
17 think I spoke with them one time before the actual
18 brief. So, like I said, I think it was a total of
19 three times altogether.

20 Q. When you say "brief," what do you mean?

21 A. Well, what I -- what I meant was just --
22 basically just explaining the process as to what to
23 expect as far as the deposition was concerned.

24 MS. LaROSS: And we want to be careful
25 here. We don't want to in any way infringe on

1 the attorney-client privilege or what was
2 discussed.

3 BY MR. CROSS:

4 Q. Did you review any documents in any of the
5 meetings or phone calls with the State's counsel?

6 A. No, I did not.

7 Q. Did they describe or identify any
8 documents for you in those meetings or calls?

9 A. No, they did not.

10 Q. Did anyone other than counsel for the
11 State and yourself participate in any of those
12 discussions?

13 A. No, not to my knowledge.

14 Q. Have you discussed today's deposition with
15 anyone other than counsel for the State?

16 A. No, I have not.

17 Q. When did you first learn that we wanted to
18 depose you in this case?

19 A. Not this past Friday, but the Friday
20 prior. On January 7.

21 Q. When you received the subpoena?

22 A. Yes, I did.

23 Q. When did you leave the Secretary of
24 State's office as an employee?

25 A. I left there January 2020. I'm sorry.

1 Yeah, January 2020, correct.

2 Q. So you've been gone about a year?

3 A. Closer to two.

4 Q. Oh, right. Yes. Trying to pretend like
5 the pandemic years have not happened.

6 And do you live at the same home address
7 now that you did when you were at the Secretary of
8 State's office?

9 A. I do.

10 Q. Did the Secretary of State's office have
11 your home address on file when you were an employee,
12 to your knowledge?

13 A. To my knowledge. I would assume they did,
14 yes.

15 Q. Do you have the same phone number now that
16 you had when you were an employee at the Secretary
17 of State's office?

18 A. Yes.

19 Q. Did anybody contact you last year letting
20 you know that we had asked to depose you as of at
21 least October?

22 A. No.

23 Q. Given the Secretary of State's office had
24 your home address and your phone number, do you have
25 any idea why the State's counsel told us just before

1 we subpoenaed you that they could not find you?

2 MS. LaROSS: I object to the form --

3 THE WITNESS: No.

4 MS. LaROSS: -- of the question.

5 And I should note, David, we are reserving
6 all objections except those going to the form
7 of the question and responsiveness of the
8 answer until trial.

9 Is that correct?

10 MR. CROSS: That's the default, yeah.

11 BY MR. CROSS:

12 Q. I'm sorry. You said the answer was "no,"
13 Mr. Oliver?

14 A. I'm sorry. I -- I -- I kind of lost -- I
15 kind of lost the question with -- with the dialogue
16 there.

17 What was the -- what was the question
18 again?

19 Q. Right. The question was, as you sit here,
20 do you know why the -- the State defendants' counsel
21 told us they could not locate you when you live at
22 the same home address and have the same phone number
23 you did when you were an employee of the State?

24 MS. LaROSS: And the same objection.

25 You may go ahead and answer, Mr. Oliver.

1 THE WITNESS: And the answer to that was
2 no.

3 BY MR. CROSS:

4 Q. What were the circumstances of your
5 departure from the Secretary of State's office in
6 January of 2020?

7 A. I was basically dismissed. And the reason
8 for the dismissal that was on my termination papers
9 was that they -- the State decided to go in a
10 different direction.

11 Q. What does that mean?

12 A. That, I cannot answer. You would have to
13 ask the State that.

14 Q. When you say "termination papers," what do
15 you mean?

16 A. Well, like I said, basically, I was
17 terminated. Basically, my services was no longer
18 required because of they -- like I said, the reason
19 that I was given was because the State desired to go
20 in a different direction.

21 Q. And when you say "papers," was there --
22 were you given something in writing that indicated
23 you were terminated and the -- and the reason?

24 A. Yes, I was.

25 MR. CROSS: Diane, we'd ask for production

1 of the termination papers.

2 BY MR. CROSS:

3 Q. Was it a termination for cause?

4 A. When you say "for cause," you mean like --
5 explain "cause."

6 Q. Yeah, good question.

7 So I -- I guess I'm trying to understand,
8 when you say that they told you they wanted to go in
9 a different direction, did they give you any
10 information as to what that meant or why that was
11 leading to your termination?

12 A. No.

13 Q. Did you ask?

14 A. Yes, I did. That's -- I did ask why, and,
15 basically, like I said, the explanation that I was
16 given was that the State decided to go in a
17 different direction. That was the extent of the
18 explanation.

19 Q. Did you have any understanding as to what
20 that meant?

21 A. Clearly, no.

22 Q. Was it a surprise to you that you were
23 terminated?

24 A. Yes, it was.

25 Q. Why?

1 A. I'm sorry?

2 Q. Why?

3 A. Why was it -- why was it a surprise?
4 Well, pretty much it was -- it was a surprise
5 because, to me, other than -- other than the -- the
6 reasoning that I was given, I had not been informed
7 or -- nor did I -- was aware of any, I guess you
8 could say, mis- -- there was nothing on my conduct
9 or job performance that I felt that justified the
10 termination, justified termination.

11 Q. When you were an employee of the Secretary
12 of State's office, did you receive periodic
13 evaluations of your performance?

14 A. For the most part, yes. Not every year,
15 but -- there was a year -- there was some that was
16 missed, but, yes, I did.

17 Q. During that time, did you receive any
18 negative evaluations before your termination?

19 A. No, I never received a negative
20 evaluation.

21 Q. Do you know if your role still exists at
22 the Secretary's office?

23 A. That, I'm not -- no, I don't. No, I do
24 not. I do not, because after I left, I basically
25 didn't try and track the performance or the

1 structure of the company.

2 Q. So you don't know whether someone filled
3 your role or took on your responsibilities?

4 A. I don't know that factually, no.

5 Q. Given the responsibilities you had, would
6 you expect that someone took those on at the
7 Secretary's office?

8 A. I would --

9 MS. LaROSS: Object to the form.

10 Go ahead, Mr. Oliver.

11 THE WITNESS: Oh. I would expect, yes.

12 BY MR. CROSS:

13 Q. Because those responsibilities were
14 important?

15 A. I felt so, yes.

16 Q. And what were your responsibilities in
17 your last position at the Secretary of State's
18 office?

19 A. Basically, I was assigned the
20 responsibilities to assess and to recommend updates
21 that would reduce or mitigate any security --
22 cybersecurity risk to the -- to the Secretary of
23 State's office.

24 Q. What was your title?

25 A. The title was security manager.

1 Q. Do you have the Exhibit Share up in front
2 of you, sir?

3 A. Are you referring to me?

4 Q. Oh, yeah, yeah. Sorry, Mr. Oliver.

5 Do you have the Exhibit Share where you
6 can pull up exhibits?

7 A. No, I don't. No, I don't. Is that a --
8 is that a separate --

9 Q. It is, but we can come back to that. Let
10 me -- the one I have, I can share. It's just one
11 page. Let me figure out how I do that. Let's see.

12 (Plaintiffs' Exhibit 1 was marked for
13 identification.)

14 BY MR. CROSS:

15 Q. Can you see this document, Mr. Oliver?

16 A. Yes, I can. A little small, but I can see
17 it, yes.

18 Q. Let me make it bigger.

19 Does that help?

20 A. Yes, it did.

21 Q. Okay. So this is a document that was
22 produced to us by a company called Fortalice.

23 Are you familiar with Fortalice?

24 A. Yes, I am.

25 Q. Did you work with Fortalice at all when

1 you were at the Secretary's office responsible for
2 cybersecurity?

3 A. Yes, I did.

4 Q. What's your understanding of Fortalice's
5 role with respect to cybersecurity at the
6 Secretary's office?

7 A. They were brought in to provide,
8 basically, security assessments and to provide any
9 solutions as far as updates or anything recommended
10 that could improve security.

11 Q. And did you work with them directly at
12 periods -- at points in time when you were there?

13 A. No, I wouldn't say directly. Basically,
14 they was a third party that was hired to provide a
15 service, and at the conclusion of that service, they
16 would provide a -- a debrief or a brief.

17 But as far as -- when you say working
18 directly with them, I didn't -- I didn't perform any
19 services collaboratively with them. We just --
20 basically, they provide the service and provided us
21 with the results.

22 Q. Did you have meetings -- well, strike
23 that.

24 You mentioned, for example, they did
25 debriefs.

1 Did you participate in any of those
2 debrief meetings?

3 A. Yes, I did.

4 Q. Did you -- was it typically part of your
5 responsibilities to participate in those debrief --
6 debrief meetings with Fortalice?

7 A. Initially, yes.

8 Q. And that changed at some point?

9 A. Yes.

10 Q. When did that change?

11 A. The -- late -- 20- -- late 2018, 2019 --
12 early 2019.

13 Q. And why did that change?

14 A. That, I'm not sure.

15 Q. So sometime around late 2018 or early
16 2019, you were no longer invited to the Fortalice
17 debriefs?

18 A. I'm going to say yes. I'm going to answer
19 that yes. And the reason I -- the reason I say that
20 is because I -- I wasn't invited to every debrief.
21 I did -- I did attend some, but not all.

22 Q. Did you ask anyone why you were no longer
23 invited to those debriefs?

24 A. Yes, I did.

25 Q. What were you told?

1 A. Basically, I really wasn't given a
2 specific reason or answer.

3 Q. Given your role as manager of
4 cybersecurity for the Secretary's office, did it
5 surprise you that you were excluded from the
6 debriefs with Fortalice, the Secretary's
7 cybersecurity outside advisor?

8 MS. LaROSS: Object to the form of the
9 question.

10 Go ahead, Mr. Oliver.

11 THE WITNESS: Yes.

12 BY MR. CROSS:

13 Q. And no one ever told you why that was?

14 A. Not definitively, no.

15 Q. What did you hear? You said "not
16 definitively." What understanding or -- did you
17 hear about why you were excluded?

18 A. Well, and the reason I said -- and the
19 reason I answered that like that, I mean, no one --
20 no one actually -- I was not in a meeting where
21 someone just told me I was not invited because of A,
22 B, or C.

23 Q. At some point they just stopped inviting
24 you but didn't tell you why; is that fair?

25 A. That's fair.

1 Q. So I have in front of you -- and we'll
2 come back. We'll talk a little more about
3 Fortalice, but in front of you is Oliver Exhibit 1.

4 And does this look to you like a fair and
5 accurate representation of the -- the organizational
6 structure of the information technology component of
7 the Secretary's office from when you were there?

8 A. From when I was there, yeah, that looked
9 fairly -- that looked fairly accurate, yes.

10 Q. And here your title is "security manager";
11 right?

12 A. That is correct.

13 Q. And do I understand right you reported
14 directly to Merritt Beaver, the CIO?

15 A. Yes, that is correct.

16 Q. And does Mr. Beaver report directly to the
17 Secretary of State?

18 A. That, I'm not sure of. Based on the
19 structure, I would think that he supported [sic] to
20 the CIO, but I'm -- again, I'm not 100 percent sure
21 of that.

22 Q. But you see --

23 A. Not the CIO, but the COO, the position
24 that's now held by Mr. Sterling, I think. I think
25 it was COO.

1 Q. I see.

2 So you think -- you think the CIO might
3 report to the COO, who then reports to the
4 Secretary?

5 A. Yes, correct.

6 Q. Why do you think that?

7 A. Well, that was just based to my -- my
8 understanding based on the organization structure
9 administratively from -- during the time that I was
10 there.

11 Q. And given that as the manager of security
12 for the Secretary's office you reported directly to
13 the CIO, is it fair to say you were in a fairly
14 senior position?

15 A. One would think, yes.

16 Q. How long were you the security manager?

17 A. I was in the position for just shy of six
18 years.

19 Q. So around 2014 to January 2020; is that
20 about right?

21 A. That is correct, yes.

22 Q. You described your responsibilities in
23 that role earlier.

24 Did your responsibilities generally stay
25 the same over the course of those six years?

1 A. Yes. For the most part, yes.

2 Q. How long did you work at the Secretary's
3 office in any capacity?

4 A. On just that -- I was in the Secretary's
5 office the entire time that I was with the State.

6 Q. Sorry. Let me ask -- ask a better
7 question.

8 Did you work for the Secretary's office in
9 any capacity other than security manager?

10 A. No.

11 Q. So the only role you ever had in the -- in
12 the Secretary's office was the six years you were a
13 security manager?

14 A. That is correct.

15 Q. Did your responsibilities as security
16 manager encompass the election system as well, the
17 security of the election system?

18 MS. LaROSS: Object as to form.

19 You can answer, Mr. Oliver.

20 THE WITNESS: Oh, okay.

21 Initially, no. At the end of my tenure,
22 there was some responsibility for elections.

23 BY MR. CROSS:

24 Q. And what was that?

25 A. Well, basically, the responsibilities for

1 the election came about once they left the Election
2 Center at Kennesaw State, which was, guesstimation,
3 somewhere around 2018 maybe. And that's -- like I
4 said, again, I'm not exactly sure what date they
5 actually transferred to the -- under the Secretary
6 of State's control, but I'm -- I'm going to just
7 take a guess and say somewhere around 2018.

8 Q. What responsibilities did you pick up with
9 that transfer from Kennesaw to the Secretary's
10 office?

11 A. Basically, the election database came
12 under the control of the Secretary of State
13 infrastructure.

14 Q. What's the election --

15 A. So --

16 Q. Sorry. Go ahead.

17 A. So, basically, that just meant kind of
18 being -- kind of having security oversight for
19 ensuring that that particular system came over as --
20 as secure as possible.

21 Q. What's the election database?

22 A. For the -- for the -- I'm going to say --
23 basically describe it from a technical standpoint.
24 Basically, a server.

25 Q. And -- and you're talking about the -- the

1 server that Kennesaw State managed previously? Is
2 that what you're referring to?

3 A. Yes, that's the one that I'm referring to.
4 But not -- not that particular hardware, but the
5 same -- the same responsibility.

6 Q. Okay. The data on that hardware was
7 transitioned to a server system at the Secretary's
8 office; is that right?

9 A. Yes.

10 Q. And then your responsibilities at that
11 point included maintaining a secure environment for
12 that data and for that system as well?

13 A. That is correct.

14 Q. Did that continue until you left in
15 January of 2020?

16 A. Yes.

17 Q. Did your responsibilities as security
18 manager also encompass in any way the security of
19 election equipment, like DREs or BMDs, scanners,
20 printers?

21 A. Under -- under the structure that I had
22 during my time there, no.

23 Q. Who was responsible during your time for
24 the security of the election equipment?

25 A. I'm -- I can't remember the name, but that

1 basically -- they still had an election -- I'm going
2 to say an Election Center. Even though it wasn't at
3 Kennesaw State, there was an Election Center or
4 office that managed that -- that equipment.

5 Q. Was that managed by Michael Barnes?

6 A. The name sounds familiar, yes.

7 Q. Did you work with Mr. Barnes?

8 A. No, I did not work with Mr. Barnes. We --
9 we had several conversations, but we were not -- we
10 didn't work together, no.

11 Q. Are you familiar with David Hamilton?

12 A. I am.

13 Q. David Hamilton was the CISO; is that
14 right?

15 A. You know, I am not sure -- I am not sure
16 what Mr. Hamilton role was. When I met
17 Mr. Hamilton, he was brought on as a contractor to
18 advise the Secretary of State and the security
19 offices on improvements or assessments of the
20 security posture of the State.

21 Q. Did you ever report to him?

22 A. No, I did not report to him, although I
23 did have -- I did work with him on that -- on -- on
24 the project that he was brought in -- where I met
25 him at. The project that he was brought in, we

1 did -- we did collaborate together.

2 Q. One quick question on Exhibit 1 here.

3 On your name, there's no one with a line
4 below you.

5 Was there anyone that reported to you as
6 security manager?

7 A. I was the -- no, I had no -- I had no -- I
8 had no -- no one reported to me. No staff, no
9 employee reported to me. I had no one working for
10 me, if that's the question.

11 Q. Was there anyone in the Secretary's office
12 that you would turn to for support to meet your
13 responsibilities?

14 MS. LaROSS: Object to the form of the
15 question.

16 Go ahead, Mr. Oliver.

17 THE WITNESS: I could -- as -- I could
18 turn to the CIO and the network team for
19 support.

20 BY MR. CROSS:

21 Q. All right. Mr. Oliver, I'm going to pull
22 up another document.

23 (Plaintiffs' Exhibit 2 was marked for
24 identification.)

25

1 BY MR. CROSS:

2 Q. Can you see this?

3 A. Yes, I can. Thank you.

4 Q. And so this is Exhibit 2.

5 And I'll just scroll through it so you can
6 take a look and tell me, does this look like a fair
7 and accurate copy of your LinkedIn profile?

8 A. You're going -- you're going rather
9 quickly, but, yeah, that basically look -- that look
10 pretty much like a copy of my LinkedIn profile. And
11 that's -- that's a living document, so it changes,
12 you know, periodically.

13 Q. So, briefly, on your education, do you
14 have a degree -- I saw you have a bachelor of
15 science.

16 Do you have a degree in computer science
17 or what's your degree in?

18 A. No. My degree -- my -- my major was
19 business, with a minor in information systems.

20 Q. So what education or training do you have
21 in cybersecurity?

22 A. I was -- in the military I was -- that was
23 my MOS in the military, security, cybersecurity, and
24 that's where -- that's where my initial training
25 started.

1 And I also had several certifications as
2 far as cybersecurity is concerned, which may not
3 necessarily be listed in that particular document
4 that you're looking at.

5 Q. Okay. So if we look in the first position
6 you have from '95 to 2007, "SAIC, Information
7 Technology Specialist," was that while you were in
8 the military?

9 A. No, that's -- that's post military. I
10 went to work for SAIC after the military as a
11 defense contractor.

12 Q. Okay. So what years were you in the
13 military?

14 A. I was in the military from '75 to '95.

15 Q. What was the highest rank that you
16 achieved in the military?

17 A. Sergeant first class.

18 Q. Was that Army?

19 A. Army, yes.

20 Q. Did you retire or how did you leave?

21 A. Yes, I retired.

22 Q. Is it fair to say it was an honorable
23 discharge?

24 A. Honorable discharge, yes.

25 Q. So your first position was SAIC, and then

1 from there you went to Emergint Technologies from
2 2007 to 2012; is that right?

3 A. Yes. And I went to Emergint based -- I
4 didn't change companies per se, but I was
5 assigned -- I was assigned due to a merger -- a
6 merger that -- I went to Emergint -- Emergint.

7 Basically, Emergint was a -- what they
8 considered a small business, and they were given a
9 particular portion of the contract that SAIC had.
10 So -- and that -- part of that contract encompassed
11 my position that I was in at the time.

12 Q. And did you have -- did you receive
13 cybersecurity training when you were at Emergint
14 Technologies?

15 A. Yes, I did.

16 Q. Did you also receive cybersecurity
17 training at SAIC?

18 A. Yes. And, basically, cybersecurity
19 training was ongoing while I was with the -- with
20 all of the companies prior to coming to the
21 Secretary of State.

22 Basically, DOD have a -- a mandatory
23 training and certification requirement for anyone
24 that's working cybersecurity within the DOD realm.
25 And I forget the exact number, but it's something

1 like DOD2707 or something like that.

2 But, basically, they have a -- they have
3 an outline as to what the minimum requirements are
4 that you must maintain in order to -- to work
5 cybersecurity as well.

6 Q. And you met those minimum requirements in
7 both positions; is that fair?

8 A. In all of the positions, yes, I did.

9 Q. So then in 2012 and 2013, you went to
10 TEKsystems in Charleston, South Carolina, at SPAWAR;
11 is that right?

12 A. Well, again, I didn't really go to
13 TEKsystems. TEKsystems -- I was still with SAIC,
14 but based on the position that I transferred to,
15 TEKsystems was the hiring agency.

16 And they were like -- you kind of like go
17 in on a temporary status or a -- I wouldn't say
18 temporary, but like a -- a -- a -- I'm going to say
19 a test status. I forget the exact acronym.

20 But, basically, like for a particular
21 period, you're on, like, a temporary -- you're like
22 a temporary employee and then you're brought on on a
23 permanent status.

24 And that was more of a procedure issue
25 than -- than anything else. It was just an

1 administrative way to go when you -- when you change
2 positions.

3 In this case, I went to a new position.
4 So I was still with the company, but I just went to
5 a different -- a different organization.

6 Q. Okay. And then in 2013 to 2014, it
7 indicates you were at SAIC.

8 But just so I have it right, it sounds
9 like from April '95, when you left the military,
10 until February 2014, you were generally with SAIC,
11 but in different positions depending on the contract
12 work that was being done for the military or for the
13 government; is that about right?

14 A. That's about right, yeah. The only -- the
15 only time that I guess you could say that I really
16 was not with SAIC, but -- but I still was with SAIC
17 based on the fact that Emergint was a subcontractor
18 of SAIC, was that time that I was actually with
19 Emergint, which was a subcontractor on the contract
20 under SAIC.

21 Q. In each of those positions, did you have
22 some responsibility for cybersecurity?

23 A. Yes. In each of those responsibilities,
24 basically, with the exception maybe of the first --
25 of the first year after leaving the military, I

1 worked in the cybersecurity space, but it was not my
2 responsibilities to actually conduct cybersecurity.

3 Basically, what I did when I -- in those
4 first year, year and a half, was to actually teach
5 cybersecurity and the -- the military system that
6 governed the control of military operations within
7 the continental U.S.

8 Q. Okay. And I forgot to ask you: You said
9 cybersecurity was -- was part of your role when you
10 were in the -- the Army for 20 years.

11 Just generally, what responsibilities did
12 you have with respect to cybersecurity then?

13 A. Well, basically, I was the -- and I'll
14 just -- I'll just kind of like recap the last -- the
15 last couple years.

16 But, basically, I was the noncommissioned
17 officer in charge of what they called the command
18 and control system. And the last couple of years
19 prior to -- prior to retiring, I worked for a
20 organization called Third -- Third U.S. Army, which
21 was the organization that handled troop movement
22 within the Middle East.

23 So, basically, kind of like just to give a
24 summary, they handled the -- the first Gulf -- well,
25 they handled everything in the Middle East, but the

1 first Gulf war was, like, one of the highlights of
2 their missions that came about while -- during my
3 time that -- while I was there.

4 So, basically, I managed -- I operated
5 the -- the system that managed those -- those assets
6 as -- as the troops deployed to that region.

7 Q. Okay. And thank you for your service,
8 Mr. Oliver.

9 A. Thank you.

10 Q. So I have in front of you now the -- the
11 description of your position at the Secretary of
12 State. I'll pull it up so you can see it. And if
13 you need me to scroll through any of this, just let
14 me know, but this is where it starts.

15 Is this a fair and accurate description of
16 your role at the Secretary of State's office over
17 the six years you were there?

18 And if you need me to scroll down so you
19 can read the whole thing, just let me know.

20 A. And if you can scroll up just a little
21 bit.

22 Yes, that's -- that's an accurate summary
23 of -- of my duties, yes.

24 Q. Okay. And the last position --

25 A. And I --

1 Q. Oh, go ahead.

2 A. No, and I -- and I should say
3 responsibilities. Not necessarily duties, but
4 responsibilities.

5 Q. Okay. And the last -- most recent
6 position you have here is at J & J Solutions as a
7 cybersecurity consultant.

8 Is that your current position?

9 A. When you say my current position, you mean
10 that I'm -- that I'm currently in today?

11 Q. Yes.

12 A. Yes, that is -- that is a current position
13 that I -- that I hold, yes.

14 Q. And you took that position -- you went to
15 J & J Solutions right after leaving the Secretary's
16 office; is that right?

17 A. Not directly after, but yes.

18 Q. Okay. Within about a month or so, it
19 looks like; is that right?

20 A. Somewhere around there, yeah.

21 Q. What are your -- well, you've got a
22 description here.

23 The description you have in Exhibit 2, is
24 that a fair and accurate description of your current
25 responsibilities at J & J?

1 A. Yes. And that -- that position is project
2 driven. So, yes, those -- again, for the -- for the
3 sake of LinkedIn, that is correct. But depending
4 on -- depending on what project I'm -- I'm on, those
5 responsibilities can change.

6 Q. All right. Does J & J -- is it a
7 consultant for, like, individuals companies that are
8 looking for cybersecurity assistance?

9 A. Yes, correct.

10 Q. And so what are some of the companies that
11 you've worked with since you've been at J & J?

12 A. Oh, wow. I've -- I've did some consulting
13 work for a company called Iman & Associates.

14 I've done some other minor -- minor
15 consultants [sic] more like for independent tax --
16 tax offices, some physician offices, and I don't
17 have a -- I don't have a consolidated list as to
18 each and every company that -- that I've worked on
19 as far as from a project perspective.

20 (Court reporter clarification.)

21 THE WITNESS: The company, it's an
22 accounting firm called Iman & Associates. And,
23 like I said --

24 COURT REPORTER: Can you spell that,
25 please? I'm sorry.

1 THE WITNESS: I-M-A-N.

2 COURT REPORTER: Thank you. That's all I
3 needed. Thank you.

4 BY MR. CROSS:

5 Q. Have you done any work for any government
6 agencies since you've been at J & J?

7 A. No, no -- no government agencies, no.

8 Q. All right. So let's come back to your
9 position at the Secretary's office briefly.

10 You indicate here that you implemented a
11 Center for Internet Security.

12 What was that?

13 A. No, no, no. No, I didn't implement a
14 Center for Internet -- I -- basically, the Internet
15 security is a -- an organization that -- I'm going
16 to say managed or -- or set security best practices
17 for the industry worldwide.

18 And, basically, what I'm saying there is
19 that I imple- -- based on those guidelines is --
20 what I implemented within the Secretary of State's
21 office is I put those control -- put those controls
22 in or attempted best to put those controls in, which
23 is kind of like information security or IT best
24 practices.

25 Q. Got it. Okay. Yeah, sorry, I misread

1 that initially.

2 And the controls and best practices that
3 you implemented with respect to the Center for
4 Internet Security, did any of that relate to
5 Georgia's election system?

6 A. The part that -- they all did. As far
7 as -- as far as the part that we took control of,
8 all of those -- all of those controls are related
9 to -- to the election system.

10 Q. And then in the next paragraph, you
11 indicate that you "also deployed vulnerability and
12 risk management solutions," and then you give some
13 examples.

14 Do you see that?

15 A. Yes, I do.

16 Q. What are vulnerability and risk management
17 solutions with respect to cybersecurity?

18 A. That would be like -- just as an example,
19 like your enterprise systems that scan for viruses,
20 that alert you of any illicit activity that's taking
21 place on a particular network or system.

22 So it basically is like a -- a scanning
23 network or a monitoring network for all systems that
24 detect viruses and malicious behavior.

25 Q. And the solutions that you're -- that

1 we're talking about, did those also extend to the
2 election system?

3 A. Yes. When -- once the election system
4 came on our purview, that is correct, yes.

5 And let me -- if I -- if I may clarify,
6 that is the election system that was connected to
7 the infrastructure, not -- not the voting systems
8 that are stand-alone systems. We did not -- they
9 were not -- they were not connected to this
10 particular system.

11 Q. What's the distinction you're drawing
12 there?

13 A. The distinction that I'm drawing there is,
14 like, the voting machines are not part of this
15 system, because they're not -- they're not connected
16 to this system.

17 Q. What part of the election system does --
18 does the -- the infrastructure system you're talking
19 about here with respect to vulnerability and risk
20 management solutions, what does that encompass from
21 the election system?

22 A. That would be like the -- and I don't
23 want -- I -- I don't want to misspeak, but,
24 basically, like the -- the My Voter's Page system --
25 I guess that would be a good way to put it -- would

1 be one of the -- would be one of the systems that
2 are there, to my knowledge.

3 But I don't -- I can't say definitively
4 which election systems that -- is under that --
5 under that -- under that umbrella because I just
6 don't remember off the top of my head, being totally
7 honest with you.

8 Q. The -- the system that you helped deploy
9 vulnerability and risk management solutions for, did
10 that include the servers that have the election
11 management software?

12 A. When you say the election management
13 software, elaborate on that for a minute.

14 Q. Sure.

15 So under the prior election system that
16 used DREs, were you familiar with something called
17 GEMS?

18 A. I'm familiar with the term, yes.

19 Q. And did you understand GEMS was the
20 election management system that sat on some series
21 of servers to -- to manage the election system with
22 the voting equipment, with the DREs?

23 MS. LaROSS: Object to the form.

24 THE WITNESS: And, again, I -- I -- I'm
25 going to have to say I don't know, because,

1 like I said, I didn't really -- I didn't really
2 work with the election systems per se. That
3 was handled by -- like I said, they would -- by
4 Kennesaw State.

5 And then when we did get the -- when we
6 did get the portions of the election system, I
7 can't definitively tell you all of the systems
8 that came over. So I -- I would be -- I don't
9 want to misspeak and tell you something came
10 over that -- that did not come over. We had
11 some that come over, but I don't -- I don't
12 definitively remember exactly what they were.

13 BY MR. CROSS:

14 Q. Okay. When you say "deployed
15 vulnerability and risk management solutions," why is
16 it important to deploy vulnerability and risk
17 management solutions in a cybersecurity environment?

18 MS. LaROSS: Object as to form.

19 THE WITNESS: So can I answer that?

20 MS. LaROSS: Yes, you may.

21 THE WITNESS: Oh, okay.

22 Basically, that's -- that's important
23 because, basically, what you're doing is you're
24 putting in controls that will reduce or
25 mitigate any bad actor from accessing the data

1 that you're trying to protect, whether it be
2 election data or any other data that's on that
3 particular infrastructure.

4 BY MR. CROSS:

5 Q. And why does it matter, from a
6 cybersecurity perspective, if a system like an
7 election system has vulnerabilities that a bad actor
8 could exploit?

9 MS. LaROSS: Objection as to form.

10 You may go ahead and answer.

11 THE WITNESS: Okay. And could you repeat
12 that question again for me, please?

13 BY MR. CROSS:

14 Q. Sure.

15 Why does it matter that a system like an
16 election system has vulnerabilities? Why does that
17 matter from a cybersecurity perspective?

18 MS. LaROSS: Objection --

19 THE WITNESS: Well, that matters because
20 you want to try and guarantee the integrity of
21 the data as best as possible and also to
22 prevent any misuse of said -- said system.

23 BY MR. CROSS:

24 Q. Why?

25 A. Why would you want to do that?

1 Q. Yes.

2 A. Well, you would want -- you would want to
3 do that to -- basically, to -- to ensure as best as
4 possible that the information that is on that system
5 is kept to the state in which you intended it to be.

6 Q. All right. If you look in front of you,
7 do you see the sentence that reads -- begins "I
8 successfully convinced..."? Do you see that?

9 A. "I successfully...." Okay. Yes, uh-huh.

10 Q. And it reads "I successfully convinced the
11 Georgia Secretary of State C Suite to enroll and
12 participate in the state's cybersecurity insurance
13 program that reduced the organization's liability,
14 influenced managers to enforce industry compliance,
15 local security policies, and adopted framework
16 requirements."

17 Do you see that?

18 A. Yes, I do.

19 Q. Did that include any components of the
20 election system that the Secretary of State was
21 managing while you were there?

22 MS. LaROSS: I object to the form of the
23 question.

24 THE WITNESS: And you've got to forgive
25 me. So, I mean, I can -- I can respond to

1 that?

2 MS. LaROSS: Yes, go ahead.

3 THE WITNESS: Okay.

4 Yes, it did.

5 BY MR. CROSS:

6 Q. Sorry. Go ahead. You said, "Yes, it
7 did"?

8 A. Yes.

9 Q. Sorry.

10 And I was going to tell you, Ms. LaRoss
11 may object -- well, she's objected. So there will
12 be objections during the course of the day. You
13 still answer the question unless she instructs you
14 not to, which should only be if it's a privilege
15 issue. So whenever you hear the objection, you can
16 go ahead and answer unless she has told you not to
17 answer.

18 MS. LaROSS: Yeah. And I'll let you know,
19 Mr. Oliver.

20 THE WITNESS: All right. Thank you.

21 BY MR. CROSS:

22 Q. And then in the next paragraph here in
23 your bio, Mr. Oliver, it reads that you "developed
24 the Incident Response Plan and led the Incident
25 Response Team."

1 You see that?

2 A. Yes, I do.

3 Q. What did that involve?

4 A. Basically, that involved designing the
5 plan and being a member of the plan, which means --
6 designing the plan, basically, is just a policy and
7 the procedures on what you do in the case of an
8 incident.

9 And the -- being a member of the team, as
10 security manager, basically, if you have an
11 incident, then you put a -- a process that you would
12 go through in order to contain any issues or make --
13 or mitigate the issue if there is one.

14 Q. The responsibilities you describe here,
15 did that also encompass the election system with
16 respect to what the Secretary was managing while you
17 were there?

18 MS. LaROSS: Object to the form of the
19 question.

20 Mr. Oliver, you can go ahead and answer.

21 THE WITNESS: Yes.

22 BY MR. CROSS:

23 Q. What is an "incident" in the context of
24 cybersecurity?

25 A. An incident in the form of cybersecurity

1 can be many things. But just to give you an
2 example, a -- a virus that gets on a desktop would
3 be an incident. That's just -- that's just an
4 example.

5 Q. So does an incident, in cybersecurity,
6 encompass identifying some sort of vulnerability
7 with a system?

8 A. It can, yes.

9 Q. And that could be, for example, like you
10 said, like you identify that malware may be on a
11 system.

12 That would be an example of a
13 cybersecurity vulnerability; is that fair?

14 A. That is fair, yes.

15 Q. Based on your experience and training,
16 would it be a sound practice to use an information
17 system, an IT system -- well, strike that. Let me
18 ask a better question.

19 Based on your experience and training,
20 would it be a sound practice to use an electronic
21 system that had known vulnerabilities without first
22 remediating those vulnerabilities?

23 MS. LaROSS: Object to the form of the
24 question.

25 You may go ahead and answer if you can,

1 Mr. Oliver.

2 THE WITNESS: And it depends on the
3 purpose of the system. There are incidents
4 where a particular system is used because the
5 technology at the time is not of such that you
6 can mitigate a particular vulnerability and the
7 system that you're -- the services that you're
8 trying to provide would still function.

9 BY MR. CROSS:

10 Q. What if it was critical infrastructure,
11 like an election system?

12 MS. LaROSS: Object to the form of the
13 question.

14 You can go ahead and answer, Mr. Oliver.

15 THE WITNESS: And, actually, it wouldn't
16 matter as far as the -- the status of the data.

17 I mean, if you -- as an example, if you --
18 if you take a hospital and they have a system
19 that manages heart patient pacemakers and
20 that -- and the developer had only developed
21 the software to function on a antiquated
22 system, well, then you still have to manage
23 that pacemaker for the patient.

24 So the vulnerability that exists in that
25 antiquated system, you can't just shut it off,

1 because you would cause -- you would terminate
2 the patient's life. So you still have to --
3 you still have to run that system with the
4 vulnerability, knowing that the vulnerability
5 is there.

6 BY MR. CROSS:

7 Q. What if the vulnerability in your example
8 was one where someone -- a bad actor could gain
9 remote access and shut down a person's pacemaker.
10 Would you continue to use that system
11 without taking measures to eliminate that
12 vulnerability?

13 MS. LaROSS: Object to the form of the
14 question.

15 You can go ahead and answer, Mr. Oliver.

16 THE WITNESS: And, again, you would -- you
17 would take whatever -- whatever steps that you
18 could to mitigate that particular
19 vulnerability, but that's not to say that you
20 can eliminate the vulnerability 100 percent.
21 You still -- you still have to maintain --
22 allow the system to be functioning, but you
23 would -- you would take whatever precautions
24 that you could to reduce -- reduce it to a
25 minimum.

1 BY MR. CROSS:

2 Q. So is it fair to say that reasonable
3 practices in the cybersecurity field expect that if
4 you identify a significant vulnerability with an
5 electronic system, that reasonable measures will be
6 taken to eliminate or mitigate that vulnerability?

7 MS. LaROSS: Object to the form of the
8 question.

9 You can go ahead and answer, Mr. Oliver.

10 THE WITNESS: And the answer would be yes.

11 BY MR. CROSS:

12 Q. During your -- looking back at your
13 responsibilities for the incident response plan and
14 team, during your time at the Secretary's office,
15 were there any incidents that arose that you were
16 involved with?

17 A. Yes.

18 Q. What were the incidents that arose --
19 cybersecurity incidents that arose while you were
20 there?

21 A. In -- I can't remember specifically the
22 incidents that arose. I mean, the -- the system's
23 automated, so it triggered -- it triggered -- it
24 triggered incident -- there -- how -- how -- how to
25 best describe it.

1 There were -- there were several incidents
2 that were triggered. Not all -- not all turned out
3 to be incidents, but as -- from -- from a reporting
4 standpoint, the -- the system -- the system would
5 alert you of a particular abnormality that it
6 detected, which, from a cybersecurity standpoint, is
7 considered an incident. And, basically, you
8 investigate -- you investigate to see if it's a
9 actual incident or if it's a non-incident.

10 So there were -- there were quite a few of
11 those that I was a part of.

12 Q. About how many would you say over the six
13 years you were there, just approximately?

14 A. Oh, wow.

15 MS. LaROSS: Object to the form of the
16 question.

17 You can answer.

18 THE WITNESS: Yeah.

19 And I really don't know, I mean, because,
20 like I said, without actually kind of like
21 refreshing myself on some of the -- on some of
22 the reports, it's hard to -- it's hard to give
23 a guesstimation.

24 BY MR. CROSS:

25 Q. Were incidents as -- would you

1 characterize them as a regular occurrence or as a
2 rare occurrence?

3 MS. LaROSS: Object to the form.

4 Go ahead and answer, Mr. Oliver.

5 THE WITNESS: And the incident -- the
6 incident that -- the incident alerting system
7 or the vulnerability system routinely alerted
8 us to certain abnormalities within the system.

9 But as far as anything turning out to
10 actually be a true incident was not that -- not
11 that often.

12 BY MR. CROSS:

13 Q. And when you say "a true incident," you
14 mean something where you -- a conclusion was reached
15 that there was an actual significant vulnerability?

16 A. That is correct.

17 Q. And when you say "not that often," did
18 that happen more than ten times over six years?

19 A. No. Based -- from what I can remember, it
20 was maybe two or three. I'd say maybe about --
21 maybe roughly around three or so that turned out to
22 actually be an incident.

23 Q. Tell me what you recall about each of
24 those three incidents.

25 A. I'm sorry. What do I recall about them?

1 Q. Yes, sir.

2 A. I -- I can -- it's hard -- it's hard to
3 say right now.

4 The only -- the only -- the only one that
5 I can actually -- well, two that I can just actually
6 say that I could recall off the top of my head, one
7 was where a particular staff member attempted to
8 plug in a USB device, which was detected, which
9 triggered -- triggered an incident because it was
10 a -- what in the cybersecurity world was called a
11 rogue -- a rogue device. And the system will alert
12 you when someone plug- -- plugs something in that
13 not typically should be allowed on the network.
14 That was one incident.

15 And the other incident that I can
16 remember, again, basically a user bringing in a --
17 bringing in a file or document and trying to access
18 it, which had a virus on it.

19 But that -- those are the -- those are the
20 only two that I can just recall right off the top of
21 my head. I mean, we got -- like I said, we got --
22 we got alerts -- we got alerted on more than just
23 those two, but I can't really recall as to exactly
24 what they -- what it was for.

25 Q. The USB incident, do you recall, was that

1 in the first half or the second half of your six
2 years?

3 A. I don't -- I don't really -- I don't
4 really recall whether it was first half or second
5 half.

6 Q. Do you know when --

7 A. Maybe midway. I'm not -- I'm not
8 really -- I'm not really certain as to the timing,
9 the exact time frame.

10 Q. Okay. Do you know whether that related to
11 any components of the election system?

12 MS. LaROSS: Object to the form of the
13 question.

14 Go ahead and answer.

15 THE WITNESS: No, it was not. It was not
16 in the election department.

17 BY MR. CROSS:

18 Q. And you mentioned another incident where
19 someone brought in a file or a document with a
20 virus.

21 Do you recall roughly when that occurred?

22 A. That was at the beginning of my -- my
23 tenure.

24 Q. And did that incident relate in any way to
25 any aspect of the election system?

1 A. No. That was prior -- that was prior to
2 the election system coming over.

3 Q. In that one, was there any conclusion
4 reached on whether malware went onto any component
5 of the Secretary's information technology system?

6 A. I'm sorry. Repeat that question.

7 Q. Yeah, sorry.

8 In the second incident involving malware,
9 do you know whether any conclusion was reached on
10 whether malware made it into any aspect of the
11 Secretary's IT system?

12 A. No --

13 MS. LaROSS: Object to the form.

14 THE WITNESS: No, it didn't.

15 And, basically, what was -- what the
16 incident was was the mere fact that the staff
17 member had plugged in an authorized device, and
18 with the system that was deployed, basically,
19 it would not -- it would not allow access to a
20 particular device without administrative -- one
21 of the administrators giving -- giving
22 permission for that device to be on the
23 network.

24 So, basically, it alerts you that the
25 device is there, and then you take whatever

1 appropriate action's necessary.

2 BY MR. CROSS:

3 Q. During your time -- well, strike that.

4 Are you aware of any time where malware
5 infected any aspect of the information technology
6 systems under the responsibilities of the
7 Secretary's office?

8 MS. LaROSS: Objection as to form.

9 You can go ahead and answer.

10 THE WITNESS: Not the entire system. I
11 mean, a particular -- a particular workstation,
12 that's -- on a particular workstation, yes.

13 Early -- early -- early on in my tenure,
14 there was a particular -- there was a -- a
15 workstation that had malware, but it was -- it
16 was not, like, at -- at a -- what we would call
17 a server level. That was a -- a -- a user
18 level.

19 BY MR. CROSS:

20 Q. What was the malware?

21 A. I don't recall exactly what the malware
22 was.

23 Q. Do you recall what type of malware it was?

24 A. Not off the top of my head, no.

25 Q. Just tell me generally everything you

1 recall about that particular incident.

2 A. Well, I mean, the only thing I recall
3 right now -- like I said, I recall the -- I -- I
4 have a -- I have a remem- -- a memory of the
5 incident happening, but it was not -- it did not
6 promulgate to any other system other than that
7 workstation.

8 So that workstation was, you know,
9 isolated and taken off of the network. That's --
10 that was, like, one of the -- one of the steps that
11 was taken to mitigate it. Basically, the user was
12 given a new -- given another system while that
13 particular system was sanitized.

14 That's -- that's pretty much the gist of
15 what happened, as best I can remember.

16 Q. The workstation that was infected, do you
17 recall what the role or responsibilities were for
18 the user who had that workstation?

19 A. Not particularly. To best my knowledge, I
20 don't -- it was -- it was, like, one of the -- just
21 one of the -- I guess you could say one of the lower
22 staff persons. I mean, it was not like -- it wasn't
23 in the election department, I do know that, but I
24 don't know what their role -- I don't know
25 specifically what their role was, no.

1 Q. Do you recall --

2 A. I don't recall what they were --

3 Q. Sorry.

4 Do you recall the name?

5 A. The name of the person?

6 Q. Yes, sir.

7 A. No, I don't.

8 Q. And you -- you said -- how, if at all, did
9 the Secretary's office confirm that the malware did
10 not make it beyond the particular workstation that
11 was infected?

12 A. Basically, like I said, there are -- there
13 are systems that are -- was put in place to
14 determine when a particular system was infected with
15 any kind of vulnerability, like -- like malware
16 or -- or anything like that. You -- you basically
17 get the alert and the system is disconnected from
18 the network.

19 Q. What steps, if any, were taken beyond
20 disconnecting the workstation to determine whether
21 the malware made it beyond the workstation?

22 A. Well, we scan -- the network was being
23 scanned daily, I mean, you know. So if a
24 particular -- if a particular vulnerability had
25 mitigated from one source to another source, you

1 would -- you would -- the system -- the system that
2 were -- that was in place was designed to -- to pick
3 those -- to pick those up.

4 And there was no detection that there was
5 any pandemic or widespread infection of a -- of said
6 network.

7 MS. LaROSS: David?

8 MR. CROSS: Yes.

9 MS. LaROSS: David, excuse me. I'm sorry
10 to interrupt you.

11 I need to double-check, but my Internet
12 is -- seems to be freezing. Could we take a
13 break now and -- to give me a chance to look at
14 that?

15 MR. CROSS: Sure.

16 VIDEOGRAPHER: The time is 9:17. We're
17 off the record.

18 (Off the record.)

19 VIDEOGRAPHER: The time is 9:26. We're
20 back on the record.

21 BY MR. CROSS:

22 Q. Mr. Oliver, before I forget, when we
23 talked earlier about the meetings and calls you had
24 with counsel for the Secretary of State's office,
25 did you first contact them or they contacted you?

1 A. They contacted me.

2 Q. And so when you received the subpoena, did
3 you contact anyone at the State's office,
4 Secretary's office?

5 A. No, I did not.

6 Q. So you got the subpoena and then at some
7 point after that, counsel for the State contacted
8 you; is that right?

9 A. That's right.

10 Q. And how did they contact you? Was it --
11 they called you?

12 A. Yes.

13 Q. Sounds like they knew where to find you
14 when they wanted to; right?

15 A. I'm sorry?

16 Q. Sounds like they knew how to find you when
17 they wanted to; right?

18 MS. LaROSS: Object to the form.

19 MR. CROSS: Yeah, I'm sure you do.

20 MS. LaROSS: Not necessary, David.

21 MR. CROSS: Yeah, I think we can agree a
22 lot here was not necessary. No reason
23 Mr. Oliver should have had to do this on a
24 holiday.
25

1 BY MR. CROSS:

2 Q. Okay.

3 MS. LaROSS: [Inaudible] for that reason.

4 COURT REPORTER: I'm sorry. I didn't hear
5 you.

6 MS. LaROSS: Yeah. Mr. Oliver had
7 requested to not have his deposition today
8 because of the holiday.

9 BY MR. CROSS:

10 Q. All right. Mr. Oliver, I'm going to pull
11 up another exhibit here for you.

12 A. Okay.

13 (Plaintiffs' Exhibit 3 was marked for
14 identification.)

15 MR. CROSS: This will be Exhibit 3.

16 MS. LaROSS: Are you pulling this up in
17 Exhibit Share, David?

18 MR. CROSS: Yes.

19 MS. LaROSS: Okay. Great.

20 BY MR. CROSS:

21 Q. But I'll share it again so you can see it,
22 Mr. Oliver.

23 So can you see Exhibit 3, Mr. Oliver?

24 A. Yes.

25 Q. You'll see at the top it says "Fortalice"

1 and then "Task Order."

2 You see that?

3 A. "Task Order" -- yes, "Task Order" and then
4 the number. Okay. Yes, I do see that.

5 Q. You see this is dated March 11 of 2021?

6 A. Yes, I do.

7 Q. And then "Deliverables," it refers to
8 "Monthly report including tasks accomplished by
9 labor category."

10 Do you see that?

11 A. Yes.

12 Q. Have you seen documents like this with
13 Fortalice before?

14 A. No.

15 Q. Did you ever review or receive any monthly
16 reports from Fortalice on their work for the
17 Secretary's office?

18 A. No, I did not.

19 Q. Were you aware that they were providing
20 any kind of monthly reports to the Secretary's
21 office?

22 A. No.

23 Q. Okay. To your knowledge, who was
24 responsible for managing the relationship with
25 Fortalice at the Secretary's office?

1 A. I'm sorry. Say that again.

2 Q. Do you know who was responsible for
3 managing the Fortalice relationship at the
4 Secretary's office?

5 A. I don't -- I don't specifically know that.
6 In the inception of that, I -- I -- I introduced
7 Fortalice to the Secretary of State's office, but
8 initially I was in the process -- in that process,
9 myself and Mr. Beavers. And then, like I said, at
10 some point I was not part of that process.

11 So I'm not sure -- I'm not sure who was
12 receiving or where was -- where the monthly reports
13 were going. I would assume it would be the CIO, but
14 I don't -- I don't know that -- I don't know that
15 for sure.

16 Q. And you said you introduced Fortalice to
17 the Secretary's office.

18 How did you do that?

19 A. Well, as you -- as I searched for
20 solutions to various services and systems to secure
21 the network, as part of my networking, Fortalice
22 became aware to me.

23 And I reached out to them to request a
24 introduction as to the services that they provide,
25 and, basically, I raised -- I raised the initial --

1 that initial introduction.

2 Q. What was Fortalice's general
3 responsibilities once they were engaged by the
4 Secretary's office, to your knowledge?

5 A. The initial engagements, to my knowledge,
6 was they were engaged to do a -- an assessment of
7 the network and basically -- when I say --
8 assessment -- basically to assess vulnerability, pen
9 tests, those kinds of IT services.

10 Q. And did that include aspects of the
11 Georgia election system?

12 MS. LaROSS: I object to the form of the
13 question.

14 You can go ahead and answer, Mr. Oliver.

15 THE WITNESS: I'm going to -- at the -- at
16 the end -- at the end, I would say yes.

17 In the initial portion, I would say maybe
18 not, because the election system at that time
19 was not under my responsibilities at that time.
20 So I don't recall if they had the
21 responsibilities to -- to assess the election
22 system during the initial involvement.

23 BY MR. CROSS:

24 Q. What responsibilities did they have with
25 respect to the election system once you became aware

1 that they were [inaudible] they were --

2 MS. LaROSS: [Inaudible.]

3 (Court reporter clarification.)

4 MR. CROSS: Yeah, sorry. Let me try that
5 again.

6 MS. LaROSS: Yeah. I'm sorry.

7 BY MR. CROSS:

8 Q. What responsibilities did Fortalice have
9 with respect to the election system at any point, to
10 your knowledge?

11 MS. LaROSS: Objection as to form.

12 THE WITNESS: To my knowledge, they would
13 have the -- they would have had the same
14 responsibilities to those portions of the
15 election system that was connected to our
16 network, would be the same as any other system
17 that was connected to our network, to basically
18 provide an assessment.

19 And if -- if a pen test or any kind of
20 testing element was involved in that particular
21 engagement, then they would have -- that would
22 have included the election system as well.

23 BY MR. CROSS:

24 Q. Did you ever receive any reports about any
25 work Fortalice did regarding the Georgia election

1 system?

2 MS. LaROSS: Objection as to form.

3 THE WITNESS: And I don't recall. I mean,
4 I received -- I received a -- I received a
5 report of engagement that they had done during
6 portions of the time that the election system
7 had been -- was under the Secretary of State's
8 control, but I don't -- I don't recall to what
9 extent.

10 BY MR. CROSS:

11 Q. What can you tell me about what you recall
12 about any work Fortalice did with respect to the
13 Georgia election system?

14 MS. LaROSS: Objection as to form.

15 THE WITNESS: Right now, it's sketchy.
16 But, I mean, I know -- I know that they did
17 some assessment work as to -- when I say
18 "assessment," as far as reviewing the --
19 reviewing the infrastructure and making
20 recommendations as to what -- what should be
21 improved or what could be improved or
22 identifying any -- any weaknesses that they
23 felt needed to be strengthened.

24 BY MR. CROSS:

25 Q. And what weaknesses, if any, did Fortalice

1 identify with the Georgia election system at any
2 point, to your knowledge?

3 A. I don't recall.

4 Q. You just can't recall specifically what
5 they were?

6 A. No, I can't recall specifically what they
7 were, no.

8 Q. What recommendations or improvements did
9 Fortalice recommend with respect to the weaknesses
10 with the Georgia election system?

11 MS. LaROSS: Objection as to form.

12 THE WITNESS: And I can't -- I can't say
13 that they recommended anything in regards to
14 the election system specifically.

15 They made recommendations as to the
16 infrastructure -- to the infrastructure, which,
17 like I said, at some point included the --
18 certain portions of the election system. But
19 it wasn't -- it wasn't -- to my knowledge, I
20 can't -- I don't recall of any specific
21 recommendations to the election system itself.

22 BY MR. CROSS:

23 Q. All right. Let me pull up the next
24 exhibit for you.

25 (Plaintiffs' Exhibit 4 was marked for

1 identification.)

2 BY MR. CROSS:

3 Q. Do you see Exhibit 4 here, Mr. Oliver?

4 A. Yes, I do. It's an email.

5 Q. Yes.

6 You see at the top this is an email that
7 Zac Davis at Fortalice Solutions sent to -- you can
8 see your name here on the "cc" line on October 26th.

9 A. Okay.

10 Q. Do you see that?

11 A. On -- October 2018. Okay. Uh-huh.

12 Q. And did you work with Zac Davis from time
13 to time in your role at the Secretary's office?

14 A. I don't recall Zac, no. He may -- he may
15 have been in -- I may have sat in on a meeting that
16 he was providing some feedback, but I don't
17 recall -- I don't recall working with him
18 specifically, no.

19 Q. Okay. So we come down to the earliest
20 email -- I'll show you the whole document so you can
21 see here at the bottom. The earliest email on this
22 thread is from Mr. Davis on October 23, 2018, to
23 Mr. Beaver, you, and others.

24 Do you see that?

25 A. Yes, I do.

1 Q. And you see here he writes right here, "We
2 have worked through the issues and messages are
3 being sent. I will let you know if we get a hit."

4 Do you see that?

5 A. I do.

6 Q. And Mr. Beaver responds "Will do."

7 Do you see that?

8 A. I do.

9 Q. And then Mr. Davis sends a follow-up
10 email, "After sending 4 more emails on Wednesday for
11 a total of five, we waited through yesterday to see
12 if we got any hits."

13 And in the last sentence of that
14 paragraph, he writes "We got one hit for the message
15 and one hit for the document (From different IPs)
16 but we did not receive any remote connections."

17 Are you with me, Mr. Oliver?

18 A. I'm with you, yes.

19 Q. And then he goes on in the next paragraph
20 "At this point, I would like to move into the
21 assumed breach phrase ASAP."

22 Do you see that?

23 A. I do.

24 Q. Do you recall what this was about?

25 A. I do -- I do not.

1 Q. You don't have any recollection of this at
2 all?

3 A. No, I do not have any recollection of
4 that.

5 Q. Do you recall any situation where
6 Fortalice was brought in to help with the -- a
7 potential or actual breach of the IT systems that
8 the Secretary handled?

9 MS. LaROSS: Objection as to form.

10 THE WITNESS: Fortalice was --
11 Fortalice -- they were brought in on -- on --
12 on occasions, but they were -- they were on
13 contract, I guess, kind of like what -- I'm
14 having some trouble with answering this
15 particular question -- they were on -- they
16 were on contract to provide consultation
17 services, as well as assist in mitigation
18 services if needed.

19 So to say that they were brought in for a
20 particular incident, I don't -- I don't recall
21 of a specific incident that they were brought
22 in. I mean, I know they were -- I know they
23 were levied on several occasions for several
24 things that may have transpired on the network.

25 But this particular incident -- this

1 particular situation here I don't recall.

2 BY MR. CROSS:

3 Q. Were you aware --

4 A. And --

5 Q. Oh, go ahead.

6 A. No, I was going to say and even though I'm
7 listed on the copy line, not -- that's not to say
8 that I was involved in this particular issue.

9 Q. Are you aware of any situation where there
10 was any suspected hack of any aspect of any
11 information technology system that the Secretary of
12 State has responsibility for?

13 MS. LaROSS: Objection as to form.

14 THE WITNESS: The answer to the -- the
15 general answer to the question would be yes.
16 There -- there were incidents that we
17 investigated where we thought there may be a
18 hack or something going on.

19 I -- and I know that they were
20 investigated and I -- I don't recall -- I -- I
21 don't recall of any particular -- or solution
22 to those investigations.

23 But the general answer would be yes.

24 BY MR. CROSS:

25 Q. Tell me everything you recall about each

1 of those incidents.

2 A. And that's -- that's -- that's kind of
3 what I alluded to. At this point, I mean, I can't
4 really -- I can't really just go back and -- and --
5 and pinpoint a particular incident, you know, in --
6 in -- in -- in the role.

7 I mean, I just -- I know that -- I know
8 that they were communicated on, like I said, for
9 some things that could possibly have been an
10 incident, but I don't recall what they were and I
11 don't recall what was done to remediate the issue.

12 Q. Do you know if anything was done to
13 remediate each and every one of those issues, or you
14 just weren't involved?

15 A. Some -- the answer to your question, I
16 don't know -- I don't recall what was -- what was
17 done to mitigate the issues. I wasn't involved in
18 every -- every incident that they were involved in.
19 I was involved in some, but I wasn't involved in
20 all.

21 Q. When was the most recent of those,
22 approximately, the best time frame you can give me?

23 MS. LaROSS: Object as to form.

24 THE WITNESS: Wow, I -- I really -- I
25 really don't -- can't recall the most recent.

1 Like I said, I mean, you know, things -- the
2 environment is a living environment. I mean,
3 it's like things are happening on a daily
4 basis, so I can't -- I don't -- I can't recall
5 specifically what happened at any particular
6 time. I mean, I -- I just don't recall at the
7 moment of -- of a -- I can't pinpoint and
8 recall a specific incident that -- that they
9 supported or collaborated on.

10 BY MR. CROSS:

11 Q. Did any of those occur after the Secretary
12 took over responsibility for the election system
13 that Kennesaw had been managing?

14 A. Yes.

15 Q. And do you recall what aspects of the IT
16 infrastructure those hack incidents involved that
17 the Secretary was managing, like the specific
18 components of that IT infrastructure?

19 A. No, I don't.

20 Q. Do you know what the conclusions were of
21 any investigations that were reached regarding those
22 concerns about a potential hack, including whether a
23 hack was successful?

24 MS. LaROSS: Objection as to form.

25 THE WITNESS: I don't recall of any

1 successful hacks of any -- of any -- of any of
2 the situations that I was involved in.

3 BY MR. CROSS:

4 Q. When you say "successful hack," what do
5 you consider a successful hack?

6 A. And when I say a successful hack, I would
7 mean that there was actually an alert triggered
8 where there was a hack or you had believed
9 something -- something triggered a -- something was
10 triggered to cause you to investigate that there was
11 or could have been a hack.

12 I don't recall of anything like that that
13 had -- that was triggered and was identified as a
14 definite hack.

15 Q. Well, there was at least the one situation
16 where malware was discovered on a -- on a
17 workstation; right?

18 MS. LaROSS: Objection as to form.

19 THE WITNESS: Yes, but malware -- malware
20 wouldn't be considered a hack.

21 BY MR. CROSS:

22 Q. Why is that?

23 A. Well, a malware is -- in the particular --
24 in this particular instance, was basically not like
25 a bad actor trying to -- to levy the system, but

1 more so of a staff member being unaware that there
2 was malware on a particular device or a file or
3 whatever, and they may have inadvertently inserted
4 that -- inserted that device or tried to access that
5 file and the malware was detected once it tried to
6 promulgate onto the -- onto a particular system.

7 Q. But you don't know how the malware got
8 onto that device; right?

9 MS. LaROSS: Objection as to form.

10 THE WITNESS: I don't -- I don't recall
11 the specific circumstances of the incident.

12 BY MR. CROSS:

13 Q. Are you aware of any incident where there
14 was unauthorized access to any aspect of the IT
15 infrastructure that the Secretary of State's office
16 manages, including the election system?

17 MS. LaROSS: Objection as to form.

18 THE WITNESS: I can't recall -- I can't
19 recall of -- I can't recall that right now, no.

20 BY MR. CROSS:

21 Q. You just don't recall one way or the other
22 whether that happened?

23 A. Right. I don't -- I can't recall whether
24 that -- whether there was or wasn't at this point.

25 Q. Okay. Who was responsible for securing

1 the voting equipment itself? So under the old
2 system, the DREs, the election management server;
3 the new system, the BMDs, printers, scanners, that
4 sort of thing.

5 A. That would have came under the Election
6 Center or the election staff, which, to my
7 knowledge, the -- the equipment was stored at the
8 Election Center --

9 Q. So that wasn't --

10 A. -- or --

11 Q. I'm sorry. Go ahead.

12 A. -- or -- or -- or a facility that was
13 controlled by the Election Center.

14 Q. Okay. Do you know whether there has ever
15 been any cybersecurity assessment done of the
16 State's voting equipment?

17 MS. LaROSS: Object as to form.

18 THE WITNESS: And the answer to that
19 question is I don't know.

20 BY MR. CROSS:

21 Q. Is that something you would have expected
22 to learn when you were manager of security at the
23 Secretary's office had it been done?

24 MS. LaROSS: David, I'm sorry. I
25 missed -- I missed that. Could you repeat it?

1 MR. CROSS: Yeah.

2 BY MR. CROSS:

3 Q. Is that something you would have expected
4 to learn about, had it been done, when you were the
5 manager for security at the Secretary's office?

6 MS. LaROSS: Objection as to form.

7 THE WITNESS: And the answer -- the answer
8 would be no, because, like I said, for a
9 great -- for a great period of that time, none
10 of the election equipment or -- or -- or
11 systems came under -- under my responsibility.

12 And when they did, I didn't -- I -- I -- I
13 didn't have the responsibility of the election
14 equipment itself.

15 BY MR. CROSS:

16 Q. And your understanding is that was with
17 the Election Center; right?

18 A. To my understanding, yes.

19 Q. Are you familiar with Frances Watson?

20 A. Yes, I am.

21 Q. Did you ever work with her?

22 A. Yes.

23 Q. And how did your role and responsibilities
24 relate to hers?

25 A. I basically interacted with her as far as

1 the investigator's -- I'm trying to think of what
2 they call it.

3 Basically, the office that she worked in
4 had a -- they had a software that I was the manager
5 of at the time, which was like the back -- the
6 Georgia and the federal background system. We
7 interacted in that regard as far as that particular
8 system and also just regular cybersecurity systems
9 within her division.

10 MR. CROSS: All right. Let me mark the
11 next exhibit.

12 (Plaintiffs' Exhibit 5 was marked for
13 identification.)

14 BY MR. CROSS:

15 Q. All right. Can you see Exhibit 5 in front
16 of you, Mr. Oliver?

17 A. Yes, I do.

18 Q. So if you look at the bottom of the first
19 page, you'll see there's an email. And I'll show
20 you -- I'll come to the bottom of the whole thing.

21 So the first email in the thread is this
22 email from Logan Lamb to Merle King on August 28,
23 2016.

24 Do you see that?

25 A. Yes, I do.

1 Q. And the subject line has "IMPORTANT" in
2 all caps and then reads "concerning the security of
3 elections.kennesaw.edu."

4 Do you see that?

5 A. Yes, I do.

6 Q. Are you familiar with the situation here
7 where Logan Lamb, an independent cybersecurity
8 researcher, identified certain vulnerabilities with
9 certain aspects of the Kennesaw server -- election
10 server?

11 A. Yes.

12 Q. Tell me what you know about that
13 situation.

14 A. Basically, I just pretty much know general
15 knowledge. I know that Mr. Lamb, if I recall
16 correctly, it was identified by the researcher and
17 it was alerted to the Kennesaw State Election Center
18 that the researcher either had -- had knowledge of
19 or had accessed some specific system that he should
20 not have been able to access or see.

21 That's -- that's pretty much the extent of
22 that particular situation that I'm aware of. Again,
23 like I said, I did not -- I did not work or
24 collaborate with the Kennesaw State Election Center.

25 Q. So did you have any involvement in the way

1 the Secretary of State's office handled this
2 particular situation involving Mr. Lamb?

3 A. No, I did not have any association with --
4 with the way that particular situation was handled,
5 no.

6 Q. So your understanding is that was handled
7 by the Election Center; is that right?

8 A. Yes, that was handled by the Election
9 Center, that is correct.

10 Q. Was there anything you did to ensure that
11 the vulnerabilities Mr. Lamb identified, that those
12 were remedied?

13 MS. LaROSS: Objection as to form.

14 THE WITNESS: And the -- the answer would
15 be a maybe. I -- I didn't actually communicate
16 in a -- a work-related capacity with the
17 Election Center.

18 In this particular incident, I didn't
19 speak with -- I -- I spoke with one of the
20 technicians at the Kennesaw State Election
21 Center, and, basically, the only thing our
22 communications involved was suggestions as to
23 what -- pretty much what -- what -- what can
24 be -- what can be done to improve -- to improve
25 a particular system.

1 Again, like I said, not -- not actually
2 working there, those conversation -- I was
3 only -- I -- I only worked in a advisory
4 capacity in that particular incident.

5 BY MR. CROSS:

6 Q. What suggestions were made?

7 A. I -- I don't recall exactly, because I
8 don't really exactly remember what -- the system
9 that Mr. Lamb revealed that had an issue.

10 And, like I said, I -- when I was talking
11 to the technician, I don't recall exactly what I
12 suggested that they do to either correct or mitigate
13 the particular issue that they had.

14 Q. Is there anything you recall about this
15 situation that you can tell me?

16 A. Other than the fact that it happened, like
17 I said, and the fact that, you know, I provided some
18 advisory information to the technical staff there,
19 that's pretty much it. This is not a system -- this
20 was, like, a handoff system to me, because it didn't
21 fall under my umbrella of responsibility.

22 Q. Do you have even a general recollection of
23 the advice that you provided regarding the
24 situation?

25 A. Not -- no, not really, because, like I

1 said, I don't really recall exactly what -- what it
2 was that -- that the issue was. I -- I vaguely
3 remember that it was a file or a system that the
4 researcher could navigate to, but I don't recall
5 what -- what was in the conversation as to what was
6 advised to do to mitigate that.

7 Q. Do you know if anything was done to
8 mitigate the vulnerabilities that were identified,
9 or you just --

10 A. That, I don't know. I don't know what was
11 done or if it was done. That, I can't answer to.

12 MS. HUFF: Excuse me, Mr. Cross. This is
13 Grace. I'm the Veritext concierge. I just
14 want to let you know that I'm here if you need
15 my help with anything.

16 MR. CROSS: Oh, okay. Thank you so much.

17 MS. HUFF: Uh-huh.

18 BY MR. CROSS:

19 Q. All right. Let me pull up the next
20 exhibit, Mr. Oliver.

21 (Plaintiffs' Exhibit 6 was marked for
22 identification.)

23 BY MR. CROSS:

24 Q. All right. Let me show you Exhibit 6.

25 Do you see Exhibit 6 in front of you,

1 Mr. Oliver?

2 A. Yes.

3 Q. Okay. And do you see this is a copy of
4 Rule 590-8-3 entitled "Security of Voter
5 Registration System" under the Georgia rules?

6 A. Uh-huh.

7 Q. "Yes"?

8 A. Yes, I see it, yes.

9 Q. And are you familiar with this rule?

10 A. No.

11 Q. Did you have -- well, let me just direct
12 you to one part of it.

13 Do you see at Subsection (b) --

14 A. Uh-huh.

15 Q. -- it reads "Security of the Voter
16 Registration System is vital to the administration
17 of elections in Georgia. As such, the system shall
18 be maintained in a manner that is consistent with
19 the following security standards."

20 Do you see that?

21 A. Yes, I do.

22 Q. And then there are 27 standards identified
23 under that subsection.

24 Do you see that?

25 A. I see that.

1 Q. And then the next subsection, (c),
2 "Assessments," reads "The Secretary of State shall
3 conduct or have conducted regular cybersecurity
4 assessments of the Voter Registration System."

5 Do you see that?

6 A. I do.

7 Q. Do you know whether those cybersecurity
8 assessments identified there were performed?

9 MS. LaROSS: Objection as to form.

10 THE WITNESS: No, I don't. I don't know
11 if they were performed or not.

12 BY MR. CROSS:

13 Q. Okay. And then if you come down to
14 Subsection (d), you see where it reads
15 "Certification of Substantial Compliance"?

16 A. I do.

17 Q. And then it reads "No later than
18 December 31 of every calendar year, the Secretary of
19 State shall certify that: A. The Voter
20 Registration System is being maintained in a manner
21 consistent with the standards set forth in
22 Subsection (b) of this rule."

23 Do you see that?

24 A. I do.

25 Q. You understand that's the 27 standards we

1 just looked at above; right?

2 A. Uh-huh.

3 Q. I'm sorry. "Yes"?

4 A. Yes, that's yes.

5 Q. And then the certification also has to
6 certify "that the standards set forth in [that]
7 Subsection (b) have been reviewed to ensure that
8 they remain generally consistent with industry
9 standards."

10 Do you see that?

11 A. I see that.

12 Q. As the manager of security for the
13 Secretary's office, did you have any responsibility
14 with respect to the certification required here?

15 A. I -- can you rephrase that?

16 Q. Sure. I'm just trying to understand --
17 there's a certification that's required under the
18 rule here that the -- the Voter Registration System
19 is being maintained in a manner consistent with
20 these 27 standards under Subsection (b).

21 What role, if any, did you have with
22 respect to the Secretary's office providing that
23 certification in any given year?

24 MS. LaROSS: Objection as to form.

25 THE WITNESS: None to little.

1 BY MR. CROSS:

2 Q. Okay. What little involvement did you
3 have?

4 A. The little -- the little part would be,
5 like I had stated before, when the portions -- when
6 certain portions of the election system became part
7 of the general Secretary of State infrastructure,
8 then I -- I did have the responsibility to ensure
9 that those systems was under -- under -- under the
10 standards, not necessarily the election standards,
11 but the standards as far as IT is concerned.

12 Q. Okay. And how did you determine that?

13 A. As far as -- as far as the systems that --
14 if they met the IT standards?

15 Q. Yes, the systems here that require
16 certification -- sorry. Strike that.

17 The standards here that require
18 certification, how did you determine whether the
19 systems that you were handling met those standards?

20 A. And, again, the particular document from
21 the election requirement, I -- I was -- I'm not
22 aware of this particular rule. So, basically, I was
23 operating from a general IT cybersecurity standard.

24 Q. Did you ever personally sign any
25 certification for the Secretary's office that it was

1 meeting particular standards -- cybersecurity
2 standards?

3 A. I don't think so, no.

4 Q. Do you know who at the Secretary's office
5 was responsible for the certification that's
6 identified here in this rule?

7 A. The answer would be, no, I don't know who
8 was responsible for that, no.

9 Q. Do you know whether the Voter Registration
10 System in Georgia actually complied with the 27
11 standards listed here while you were there?

12 A. Again --

13 MS. LaROSS: Objection as to form.

14 THE WITNESS: Again, I'm not -- I'm not
15 familiar with the rule, so I can't -- I can't
16 say that I am aware that they did or didn't.

17 BY MR. CROSS:

18 Q. Okay. Did anyone at any point ever
19 threaten to hack Georgia elections? Are you aware
20 of any such --

21 MS. LaROSS: Objection.

22 THE WITNESS: And I'm sorry, sir. Can you
23 repeat that question?

24 BY MR. CROSS:

25 Q. Sure.

1 Are you aware of any incident where
2 someone contacted the Secretary -- the Secretary of
3 State's office and threatened to hack Georgia
4 elections?

5 MS. LaROSS: Objection as to form.

6 THE WITNESS: The answer would be, no, I
7 was not made aware of any particular threat
8 where someone actually physically contacted the
9 Secretary of State's office and threatened to
10 hack any -- any portion of the system.

11 BY MR. CROSS:

12 Q. If something like that happened, would
13 that fall under your responsibilities or would that
14 fall to the Election Center or something else?

15 A. If something like that happened, it should
16 have fell under both. The -- the owner of the data,
17 that -- that being the election system, as well as
18 the -- myself as being the security manager, it
19 should have fell under both -- under both umbrellas.

20 Q. And what would be the protocol, if
21 something like that happened, to respond to such an
22 incident?

23 A. In general or in -- you're talking about
24 at the Secretary of State's office what was the
25 protocol?

1 Q. Yes. Sorry. Thank you. That's a good
2 clarification.

3 A. When a -- when a -- that -- that process,
4 I'm going to say, was a divided process, I guess
5 would be the correct answer.

6 Q. And just walk me through what that process
7 would entail, to your knowledge.

8 A. Well -- and I answered that the way that I
9 did because, again, I was not privy to all of the --
10 I was not involved in all the communications in that
11 regard.

12 But the -- the ones that I were involved
13 in, to the best of my ability, met -- met whatever
14 standards that was -- I was operating under at the
15 time. And that, for the most part, was the general
16 security, not necessarily trying to meet any
17 particular compliance or...

18 Q. So what I'm trying to understand,
19 Mr. Oliver, is if the Secretary's office received a
20 direct threat of a hack to the election system --

21 A. Uh-huh.

22 Q. -- what would be -- what policies and
23 protocols are in place for responding to that?

24 A. There -- the incident response -- the
25 incident response team or the incident response

1 policy should have been invoked. And that would
2 have been notifying the incident response team, and
3 then that -- that team been a part of the process to
4 make a determination as to what should or should not
5 be done on a particular incident.

6 Q. Who was on the incident response team?

7 A. Myself, for one; Mr. Beavers, as CIO, was
8 another; Mr. Clark Rainer, which was the information
9 technology manager; and some other network --
10 network staff persons, as well as the legal -- there
11 was a legal component to it as well. I think it was
12 Mr. Germany.

13 Q. Okay. And can you just walk me through
14 the steps?

15 So if that type of incident occurred, what
16 does the incident response protocol provide that are
17 the specific steps that would be taken by the
18 Secretary's office in response?

19 MS. LaROSS: Objection as to form.

20 THE WITNESS: And I -- I don't recall
21 exactly what the -- the incident response laid
22 out step by step, basic.

23 But in general, like I said, basically,
24 the incident response team should be notified,
25 and then within -- within the incident response

1 itself, it lay out the notification steps as to
2 who should be notified. Not necessarily what
3 action they should take, but at least who
4 should be notified. It doesn't -- it doesn't
5 really give a particular action as to, "You
6 gotta do this, you gotta do that," but the
7 response plan is mostly a roadmap that's
8 telling you who to contact and what immediate
9 action to take if it's -- if it's on a system
10 internal.

11 BY MR. CROSS:

12 Q. All right. Mr. Oliver, take a look at
13 Exhibit 7.

14 (Plaintiffs' Exhibit 7 was marked for
15 identification.)

16 BY MR. CROSS:

17 Q. Can you see this?

18 A. Yes, I do.

19 Q. And do you see at the top there's an email
20 from Kevin Rayburn to Mr. Beaver, Mr. Clark Rainer,
21 Chris Harvey, and yourself, with a cc to Ryan
22 Germany.

23 Do you see that?

24 A. Yes, I do.

25 Q. And this is sent on April 5 of 2019;

1 correct?

2 A. The date on it is, yes, correct, April 5,
3 2019. Yes.

4 Q. And it's just one page, so you can see the
5 whole exhibit here.

6 If you come down to the first email in the
7 thread, do you see that it's from an email address
8 Bret Hadley?

9 Do you see that?

10 A. Yes, I do.

11 Q. Do you see that the actual address is
12 bretsolid@gmail.com?

13 A. Yes, I do.

14 Q. And it's sent April 4, 2019; correct?

15 A. April 4, 2019, that is correct.

16 Q. And then the recipient is
17 soscontact@sos.ga.gov.

18 Do you see that?

19 A. I see that.

20 Q. Are you familiar with that address at the
21 Secretary's office?

22 A. Yes, I'm vaguely remember- -- familiar
23 with that address.

24 Q. Is that some sort of general public
25 address that people can use to contact the Secretary

1 of State's office?

2 A. Yes. That would be a -- kind of like a --
3 the answer's, yes, a general address where they can
4 contact the Secretary of State, yes.

5 Q. Kind of like -- kind of like a customer
6 service email address for a company?

7 A. That is correct.

8 Q. And the subject here in this email reads
9 "I bet I can hack your electronic voting machines."
10 Do you see that?

11 A. Yes, I do.

12 Q. And then the message itself reads "If you
13 don't want me to try and hack your elections, please
14 follow Oregon's lead and vote by mail, on paper.
15 You really DON'T" -- "DON'T" is in all caps -- "need
16 electronic voting machines, but if you insist, then
17 let the games begin. Fair warning," and it's signed
18 "Mr. Robot."

19 Do you see that?

20 A. I see that.

21 Q. Does this refresh your recollection that
22 there was at least one incident where someone
23 specifically threatened to hack Georgia election
24 machines?

25 MS. LaROSS: Objection to form.

1 BY MR. CROSS:

2 Q. You can go ahead.

3 A. Again -- again, it -- it refreshes my
4 memory to a degree, but when it came to the election
5 systems itself -- I guess that would be a -- a good
6 way to state this -- I was not responsible -- it
7 was -- I was not given that responsibility for
8 the -- for the election system.

9 So unless there was a specific threat to
10 the system that came under my purview, I would not
11 have acted on this. So, I mean, if they -- if they
12 were -- if they were alleging to -- alleging to the
13 Election Center or some type of election equipment,
14 that would have been -- that would have been handled
15 by the Election Division or the Election Center, the
16 way -- the way that daily operations went within the
17 IT department or -- at the Secretary of State's
18 office during my tenure.

19 Q. So you're one of the people that received
20 notice of this threat.

21 What involvement did you have with
22 resolving this or addressing it?

23 MS. LaROSS: Objection as to form.

24 THE WITNESS: To my knowledge, like I
25 said, I don't recall this really, really being

1 on my radar.

2 Again, like I said, I -- I may have been
3 on the email cc protocol, but I was not -- I
4 was not looped in to the main resolution of
5 this particular issue or -- or -- or -- or
6 the -- or the Election Center itself.

7 BY MR. CROSS:

8 Q. Tell me everything you remember about this
9 incident.

10 A. I don't. Actually, I mean, now that
11 you -- now that I'm looking at the document and kind
12 of recalling the incident, there -- Mr. Rayburn may
13 have said something to the IT department. I don't
14 recall him saying anything to me specifically. Not
15 to say that he didn't, but I don't recall -- I don't
16 recall him coming to me individually or -- or -- or
17 in a group form in regards to this particular
18 threat.

19 Q. So as you sit here, you just don't know
20 one way or the other what, if anything, was done in
21 response to this.

22 A. I don't -- I don't know one way or the
23 other if anything was done to that. I don't recall
24 being specifically involved in any investigation in
25 regards to this threat.

1 Q. So the -- the threat indicates that if the
2 State continues to use electronic voting machines,
3 the writer writes "...then let the games begin,"
4 indicating that they will actually try to hack the
5 voting machines.

6 Georgia did continue using electronic
7 voting machines, and has since April of 2019;
8 correct?

9 A. I'm sorry. Repeat that question again
10 now.

11 Q. You're aware that Georgia has continued
12 using electronic voting machines in the state since
13 receiving this threat; right?

14 MS. LaROSS: Objection as to form.

15 THE WITNESS: I see the -- I see the date
16 of the threat, and I -- I am aware that Georgia
17 used electronic voting machines. But the
18 voting machines -- and when you're talking
19 about the machines that the constituents
20 actually vote on -- are not to be on the
21 Internet ever.

22 BY MR. CROSS:

23 Q. But as you sit here, you don't have any
24 information you can provide on what efforts occurred
25 with respect to this hack, right, whether the hack

1 occurred, what response there was, anything like
2 that; is that right, sir?

3 A. That is correct, sir.

4 MS. LaROSS: Object as to form.

5 BY MR. CROSS:

6 Q. You said the voting machines are never
7 supposed to be on the Internet.

8 Do you know whether any of the voting
9 equipment that's currently used in Georgia has ever
10 been connected to the Internet, or you just don't
11 know one way or the other?

12 A. I don't know one way or the other.

13 Q. Are you aware of whether the election
14 management server that the Secretary of State
15 manages for the existing Dominion voting equipment,
16 are you aware of whether that's supposed to be air
17 gapped?

18 MS. LaROSS: Objection as to form.

19 THE WITNESS: And just in the general
20 state of the question, I would say, yes, that
21 it should be air gapped.

22 BY MR. CROSS:

23 Q. And what does "air gapped" mean in the
24 cybersecurity context?

25 A. Basically means that it doesn't -- it

1 doesn't have access to the general Internet, meaning
2 that my -- my son sitting at home should not be able
3 to go on the Internet and access that system by any
4 means.

5 Q. Do you know whether the election
6 management server that the Secretary of State has
7 is, in fact, air gapped?

8 A. I -- I don't -- I don't recall.

9 Q. Okay. To ensure that it's air gapped, it
10 would have to be completely detached, disconnected
11 from other parts of the IT infrastructure that the
12 Secretary manages that do have Internet connections;
13 right?

14 MS. LaROSS: Object as to form.

15 THE WITNESS: In theory -- in theory, that
16 is correct, yes.

17 BY MR. CROSS:

18 Q. Okay. And given that you were the manager
19 for security and managed significant aspects of the
20 IT infrastructure, wouldn't you need to be involved
21 to ensure that the election management server itself
22 is air gapped?

23 MS. LaROSS: Objection as to form.

24 THE WITNESS: In general -- in general
25 theory, that should -- that would be correct,

1 yes.

2 BY MR. CROSS:

3 Q. But do I understand correctly you were not
4 involved in any efforts one way or the other to
5 determine whether that -- that server is air gapped;
6 is that right?

7 MS. LaROSS: Objection as to form.

8 THE WITNESS: To my knowledge, no.

9 BY MR. CROSS:

10 Q. Okay. All right. Let's take a look at
11 Exhibit 8, Mr. Oliver. I'll pull it up here in just
12 a moment.

13 (Plaintiffs' Exhibit 8 was marked for
14 identification.)

15 MR. CROSS: And by the way, I'm happy to
16 take a break whenever you want. I was going to
17 keep going because I want to get you out of
18 here as quickly as we can on a holiday, but if
19 you want to take a break, just say the word.

20 THE WITNESS: All right.

21 MR. CROSS: All right. Let me share this.
22 This is all a lot easier when you're in person.

23 BY MR. CROSS:

24 Q. All right. Can you see Exhibit 8 here?

25 A. Yes, I see Exhibit 8, yes.

1 Q. Okay. And Exhibit 8, you see this is an
2 email that Clark Rainer sent on October 30, 2019,
3 internally at the Secretary of State's office?

4 A. Yes.

5 Q. And you see you're one of the recipients
6 in the "cc" line?

7 A. Yes.

8 Q. Okay. And then it begins with this email
9 from elections@msisac.org on October 28, 2019.

10 Do you see that?

11 A. I see that.

12 Q. Are you familiar with that organization?

13 A. I am.

14 Q. What is it?

15 A. Basically, it is a -- I don't want to say
16 a federal -- but an independent organization that
17 provides standards for -- elections standards
18 throughout the continental U.S.

19 Q. You see here it reads in the first
20 sentence of the alert, "EI-ISAC is opening the
21 Election Cyber Situational Awareness Room to state
22 and local election offices for the duration of the
23 November 5, 2019 General Election."

24 You see that?

25 A. I see that.

1 Q. And then if we come up to Mr. Rainer's
2 email, the second paragraph, he indicates "Our
3 offices -- our office serves at the point for all
4 city and county governments who are EI-ISAC members,
5 and having this portal up from Monday through
6 Wednesday will give us visibility into any
7 threats --"

8 A. I'm sorry. Where are you reading -- where
9 are you reading that at?

10 Q. I'm sorry. This -- you see here in the
11 second paragraph (indicating)?

12 A. Okay. Okay.

13 Q. So he goes on to say "...having this
14 portal up from Monday through Wednesday will give us
15 visibility into any threats being reported
16 throughout the state and country."

17 Do you see that?

18 A. I do.

19 Q. And what can you tell me about what this
20 portal is and the -- the situational awareness room
21 that's set up for elections like this, including in
22 Georgia?

23 A. Kind of -- kind of without -- like I said,
24 my memory is kind of vague, but, basically, it is
25 a -- kind of like a cyber war room that's set up,

1 typically, at the -- I'm going to say the GBI, but I
2 might be -- I might be incorrect in that. But -- I
3 think it's the G- -- I think it's ran by the GBI,
4 but don't -- like I said, I don't want to -- I don't
5 want to say that.

6 But, basically, there's a record -- a
7 cyber room that's managed by one of the law agencies
8 that set up a war room of various governments,
9 whether it be county, city, or whatever, to come
10 together and kind of like -- kind of like what they
11 call a SOC.

12 But, basically, all of the threat analysis
13 come into -- are -- are being fed to this particular
14 location, and they can look at and analyze any
15 particular threat and issue a warning or instruct
16 someone to take action on a particular issue that
17 they may or may not see.

18 Q. Is at least part of the idea that if
19 another state, for example, experiences some threat
20 to their election, they can share that information
21 with cybersecurity folks in other states so that
22 everyone has an understanding of what sort of
23 threats may be happening? Is that part of the --

24 A. Yes, that's -- that is part of it, yes.

25 Q. What was your involvement, if any, with

1 this particular process?

2 A. I had -- I had some involvement, but
3 because of the -- basically, just because of the --
4 when you looked at -- if you go back to -- think
5 back to the organization chart, I had a -- I had a
6 department of myself. So my -- my involvement was
7 only supported to the limits that one can -- one can
8 be present for.

9 Q. What threats do you recall learning about
10 in your work with this organization on election day?

11 MS. LaROSS: Objection as to form.

12 THE WITNESS: Yeah, and I -- I can't
13 really -- I can't really say that I can recall
14 any particular threat that was identified
15 relating to the state of Georgia on election
16 day.

17 (Plaintiffs' Exhibit 9 was marked for
18 identification.)

19 BY MR. CROSS:

20 Q. All right. Let's take a look at
21 Exhibit 9.

22 A. Okay.

23 Q. Can you see Exhibit 9, Mr. Oliver?

24 A. I do.

25 Q. You see this is an email from John Hallman

1 sent on July 3, 2019, at the Secretary's office?

2 A. Yes.

3 Q. And you see that you're the first in the
4 list of recipients there.

5 Do you see that?

6 A. I see that.

7 Q. And the other recipients are Merritt
8 Beaver, Chris Harvey, Kevin Rayburn, and Scherie
9 Jefferies; is that right?

10 A. Uh-huh.

11 Q. Is that "yes"?

12 A. Yes, that is a yes.

13 Q. Who is Scherie Jefferies?

14 A. Scherie Jefferies is a -- she's an
15 employee of the Secretary -- well, she -- at the
16 time I was there, she was an employee of the
17 Secretary of State IT department.

18 Q. So we come down -- the first email in the
19 thread here is from John Hallman on July 3, 2019, to
20 you, Mr. Beaver, Mr. Harvey, and Mr. Rayburn.

21 Do you see that?

22 A. I see that.

23 Q. And the subject is "Cloudflare Email
24 Obfuscation."

25 Do you see that?

1 A. Uh-huh, I see that.

2 Q. Mr. Hallman writes to you and Mr. Beaver
3 "I began receiving reports at the beginning of April
4 that County registrars were unable to view the email
5 address saved in ElectioNet."

6 Do you see that?

7 A. I see that.

8 Q. What is ElectioNet?

9 A. Well, it's one of the election system.
10 Like I said, you gotta forgive me. I'm trying to
11 recall. But, basically, I'm thinking that it's a --
12 I'm thinking that it's a system where the counties
13 can view various voter information. And voter
14 information may be -- let me rephrase that. Not
15 necessarily voter information, but it's like -- I'm
16 going to say stats for a particular county.

17 But I don't -- I'm -- I'm -- I -- again,
18 I -- I didn't really work in elections. I'm
19 familiar with the ElectioNet. I know what the
20 network is. I can't really specifically tell you
21 all of what it does.

22 Q. Okay. ElectioNet is sometimes referred to
23 as ENET; right?

24 A. I would -- I would assume, yes.

25 Q. And you see here it indicates "The user,"

1 meaning someone at the County office, "The user
2 would see 'Email Protected' in the place of the
3 email address, and this message would be a
4 hyperlink."

5 You see that?

6 A. I see that.

7 Q. And then "Clicking on this link, would
8 take the voter to a webpage informing the user that
9 Cloudflare was preventing them from seeing the email
10 address."

11 Do you see that?

12 A. I see that.

13 Q. And then it goes on in the next paragraph.
14 "Over the next 3 months, our IT department
15 investigated the cause of the issue, which appears
16 to be a feature of Cloudflare called Email Address
17 Obfuscation. It was determined that this is a
18 setting that can be turned off."

19 Do you see that?

20 A. I see that.

21 Q. He then goes on to explain, "However, when
22 we requested that this setting be turned off, that
23 request was denied by the two of you. Could you
24 please explain this to me?"

25 Do you see that?

1 A. I see that.

2 And, again, in my limited memory,
3 basically, Cloudflare was a -- a service that we
4 were utilizing to limit or detect any suspicious
5 transactions over the mail system and, by turning
6 that on, would have disabled that protection.

7 So to the best of my recollection, that
8 was why it was denied. Because even though it
9 prevented some services -- it prevented the easy
10 flow of services, it was a -- it was a protection
11 that was recommended for the safety of the network.

12 Q. Recommended by whom? You and Mr. Beaver?

13 A. Yes. And not -- I won't say -- it was in
14 this particular case recommended by me and
15 Mr. Beavers, but it was recommended based on the
16 Cloudflare recommendations and the way that
17 Cloudflare operates.

18 Q. So you think this was a recommendation
19 from Cloudflare itself?

20 A. It was a recommendation from Cloudflare
21 itself. But even though -- even though it's a
22 recommendation from Cloudflare, you have to keep in
23 mind that Cloudflare provides services to all 50
24 states, basically.

25 And each state network is configured

1 differently, so what is feasible in one state may
2 not be feasible in another state. And the way that
3 we were constructed, this provided us the best
4 solution possible at the time.

5 Q. Okay. So you should see in front of you
6 here your response to Mr. Hallman on July 3, 2019.

7 Do you see that?

8 A. I do.

9 Q. And if you go to the third sentence
10 beginning "Turning...."

11 Do you see that at the end of the second
12 line?

13 A. Uh-huh. Right.

14 Q. And you wrote "Turning this feature does
15 create a security vulnerability, yes we can restrict
16 this to the Electionnet [sic] site but this is one
17 of the organizations [sic] critical sites."

18 Do you see that?

19 A. I do see that.

20 Q. So you're indicating to Mr. Hallman that
21 turning this feature off would create a security
22 vulnerability; is that right?

23 A. To the best I can --

24 MS. LaROSS: Object to the form.

25 THE WITNESS: -- the best -- go ahead.

1 I'm sorry.

2 MS. LaROSS: Go ahead, Mr. Oliver.

3 THE WITNESS: To the best I can recall,
4 and, again, without being -- not being in the
5 moment, to the best of my knowledge, I would
6 say, yes, that would be correct.

7 BY MR. CROSS:

8 Q. And then Mr. Hallman asked you in his
9 response on the same day if you could explain the
10 security vulnerability that will be created by
11 turning this feature off.

12 Do you see that?

13 A. I see that.

14 Q. What is the security vulnerability that
15 would be created by turning this feature off, in
16 your view?

17 A. I really -- I really don't know at this
18 point. At the time, you know, I was abreast of what
19 that particular feature was protecting. At this
20 point, it's a -- it's a -- it's a -- it's a fog in
21 my mind. I can't remember what -- what was being
22 protected at the time or what turning it off would
23 have -- what vulnerability it would have presented.

24 Q. Okay. Do you know whether it was ever
25 turned off?

1 A. That, I do not know.

2 Q. Okay. And when you wrote to Mr. Hallman
3 here in your email "...we can restrict this to the
4 Electionnet [sic] site but this is one of the
5 organizations [sic] critical sites," what did you
6 mean was one of the organization's critical sites?
7 Was that ElectioNet?

8 A. I don't -- I don't really recall as to
9 what I meant specifically in that -- in that -- in
10 that email.

11 Q. Is ENET considered one of the Secretary's
12 critical sites?

13 A. I would -- I would --

14 MS. LaROSS: Objection --

15 THE WITNESS: -- assume it was -- I would
16 assume it was at the time, yes.

17 COURT REPORTER: Ms. LaRoss, you might
18 want to repeat your objection. It was cut off.

19 MS. LaROSS: Yeah. Objection as to form.

20 Thank you.

21 BY MR. CROSS:

22 Q. Are you familiar with an organization
23 called Secureworks?

24 A. Yes, I am. Secureworks is a division of
25 Dell Enterprises.

1 Q. A division of what Enterprises?

2 A. Dell Enterprises.

3 Q. Is that D-A-L-E?

4 A. No. D-E-L-L, Dell, like the computer
5 Dell.

6 Q. Oh, Dell. Sorry. Got it.

7 A. Yes.

8 Q. Okay. And did the Georgia Secretary of
9 State's office have some relationship with
10 Secureworks?

11 A. They did.

12 Q. What was that?

13 A. Secureworks was just like a -- they
14 provide like a third-party SOC service.

15 Q. Did they provide reports based on --

16 A. Yes, they did.

17 Q. How frequently did they provide those
18 reports?

19 A. Daily.

20 Q. Daily, you said?

21 A. Yes, daily.

22 Q. And those reports included cybersecurity
23 assessments?

24 A. Not assessments, no. It wasn't -- it
25 wasn't an assessment. It provided information

1 for -- for assessment, but it was not a -- an
2 assessment. They did not do assessment. It just
3 provided information that led to assessments. It
4 was one of the pillars.

5 Q. What -- what was -- just help me
6 understand, what was in the daily reports,
7 generally?

8 A. Well, it was -- it was -- it was a
9 canned -- a set of canned reports. And what I mean
10 by that is you can -- the user, whomever that be,
11 can set up to have whatever report they deem
12 important to them to be delivered or they can run --
13 or they can run it a la carte.

14 So as an example, if I wanted to see all
15 of the IPs that were reporting to a particular
16 system, I could -- I could run a report on demand
17 and get that information, or I could set it up where
18 it automatically ran that report and sent it to my
19 email on a daily, monthly, or semi- -- semi-monthly,
20 quarterly, whatever -- whatever interval that I so
21 desired.

22 Q. Okay. Did these reports include any
23 information on security vulnerabilities with the
24 system?

25 A. They could, yes.

1 Q. If there was any kind of breach of the
2 State's electronic systems, would that be
3 captured -- would you expect that to be captured in
4 these reports?

5 MS. LaROSS: Objection as to form.

6 THE WITNESS: In -- in general, yes.

7 BY MR. CROSS:

8 Q. Okay. All right. Let me share
9 Exhibit 10.

10 (Plaintiffs' Exhibit 10 was marked for
11 identification.)

12 BY MR. CROSS:

13 Q. Do you see this, sir?

14 A. Yes, I do.

15 Q. Okay. And do you see the most recent
16 email at the top is from Josh Hood to a number of
17 people at the Secretary of State's office on April 3
18 of 2019?

19 A. I do see that, yes.

20 Q. And you see you're one of the recipients
21 in the "cc" line?

22 A. I do see that, yes.

23 Q. Okay. And Josh Hood's email indicates
24 he's at ellijay, E-L-L-I-J-A-Y, .com.

25 Do you see that?

1 A. I see that.

2 Q. And if you look at his signature block,
3 "Professional Services Tech, ETC," what's ETC?

4 A. That, I am not aware of.

5 Q. Okay. All right. If we come down to the
6 start of this, you'll see there's an email from
7 Clark Rainer to Steven Koonce at the Secretary of
8 State's office April 3, 2019, subject line "Fannin
9 County IP."

10 Do you see that?

11 A. I do see that, yes.

12 Q. And Fannin County, is that a county in
13 Georgia?

14 A. Yes, it is.

15 Q. What was Steven Koonce's role around this
16 time?

17 A. Mr. Koonce was part of the network team.

18 Q. And you see there's this IP address that's
19 included in Mr. Rainer's email. Mr. Koonce sends a
20 response indicating, "This is one of several blocks
21 from this morning."

22 Do you see that?

23 A. I see that, yes.

24 Q. And do I read this right that it indicates
25 they're blocking this IP address in Mr. Rainer's

1 email?

2 A. Yes, based on -- looks like that's what
3 they're doing based on this -- on this portion of
4 the report that's in the email, yes.

5 Q. Okay. And in this portion of the report,
6 you can see the same IP address listed and then it
7 says "Action taken: Block."

8 Do you see that?

9 A. I see that, yes.

10 Q. Under "Rule name," it says "Block High
11 Threats."

12 Do you see that?

13 A. I see that, yes.

14 Q. Is that just a rule that's intended to
15 block IP addresses that are perceived to be a high
16 threat?

17 MS. LaROSS: Object as to form.

18 THE WITNESS: Again, depending on what
19 you're trying to accomplish. The rule can
20 block anything from a high threat to something
21 that you may want to just flag for whatever
22 reason.

23 Not necessarily saying that it's a threat,
24 but if you wanted to flag it or if you wanted
25 to manually allow or disallow a particular IP,

1 you can -- you can set up a -- a rule to do
2 that.

3 BY MR. CROSS:

4 Q. Okay. And then we come to a more recent
5 email, still on April 3, 2019, from Mr. Koonce
6 regarding the same IP address. It indicates "There
7 have been 66 times this rule has been triggered from
8 the IP address in question the last three days."

9 Do you see that?

10 A. I see that, yes.

11 Q. And there's another email the same day
12 from Mr. Rainer to Josh Hood, the person we saw
13 earlier who was at ETC.

14 Do you see that?

15 A. I see that.

16 Q. And he indicates in the second paragraph
17 to Mr. Hood, "We have identified the IP address and
18 the url fannincountyga.com as appearing on a number
19 of blacklists and potential reasons for this may
20 be:"

21 Do you see that?

22 A. I see that.

23 Q. And Mr. Hood responds "This is the first
24 notifications I have had on this. I will look into
25 it and update you on what I find."

1 With me?

2 A. I see that, yes.

3 Q. What do you recall about this situation?

4 A. I don't. As far as the flow of the email,
5 I understand what they're talking about, but I don't
6 recall this particular situation.

7 Q. Okay. You don't recall anything about
8 this "fannincountyga" IP address?

9 A. I -- I remember there being an issue with
10 Fannin County. And when I say an "issue," I'm
11 talking about where something like this happened
12 where a particular user or -- or system, something
13 like that, contacted our office and asked us to look
14 into something or something like that.

15 I do remember something like that with
16 Fannin County, but I don't recall the details of
17 what they were -- what they were asking or what we
18 did to resolve their situation.

19 Q. Do you know whether any conclusion was
20 reached that the IP address here is not actually
21 associated with Fannin County in Georgia, whether
22 someone was pretending to be with Fannin County?

23 A. I do not recall specifically what the
24 resolution was on that.

25 The only thing that I can really add to

1 that is that when Mr. Rainer was referring to that
2 it -- it could be part of a bad IP, basically,
3 there's -- there's a MS -- MS -- MS-ISAC -- and I
4 forget what the acronym stands for -- but,
5 basically, they're like the government agency that
6 monitors IP sectors in the United States and
7 anything that's malicious.

8 And, basically, they send out a -- a list
9 of IPs that has been identified as a malicious IP or
10 the potential thereof, and you can add those to a
11 firewall or a email or protection system to flag or
12 block a particular IP.

13 And that's what appeared to be happening
14 here, is that a particular IP that they're referring
15 to was either flagged or blocked totally.

16 Q. Would you expect a legitimate IP address
17 associated with a Georgia county to be flagged and
18 blocked in that way?

19 A. It's possible, yes.

20 MS. LaROSS: Object as to form.

21 BY MR. CROSS:

22 Q. Why is that?

23 A. Well, depending on -- again, these --
24 these systems are monitored -- a great part of them
25 are monitored automatically. And depending on the

1 normality of the traffic that's being detected, if
2 it's out of range of what the filter is set up to
3 filter on, if it's out of that range, then it could
4 be flagged as a malicious -- a malicious IP or a
5 malicious activity.

6 Q. In the reasons given in Mr. Rainer's email
7 to Mr. Hood of why the fannincountyga.com is
8 appearing on a number of blacklists, the last reason
9 indicates that Mr. Rainer had "just got an email
10 from MS-ISAC" --

11 A. MS-ISAC. Okay.

12 Q. -- "with some more information" he
13 indicates he'll forward on in just a minute "also
14 showing you may have a malware infection."

15 Do you see that?

16 A. I see that, yes.

17 Q. And was there, in fact, a malware
18 infection in this incident?

19 MS. LaROSS: Object --

20 THE WITNESS: I don't recall.

21 BY MR. CROSS:

22 Q. You just don't recall one way or the
23 other?

24 A. I don't recall one way or the other,
25 correct.

1 Q. Okay. Do you recall any measures that
2 were taken to investigate whether malware had made
3 it into the Secretary of State's system?

4 A. The answer would be no, but in general
5 practice, we would -- we would investigate that
6 based on -- on operating standards. But I don't
7 recall specifically if anything was -- any
8 additional action was taken for this particular
9 issue.

10 COURT REPORTER: Ms. LaRoss, please
11 restate your objection. I didn't hear it.

12 MS. LaROSS: Objection as to form.

13 BY MR. CROSS:

14 Q. Do you know why Mr. Rainer reached out to
15 Josh Hood at ETC about this instead of reaching out
16 to someone at Fannin County?

17 A. I would -- I don't know for sure, but I
18 would assume since Mr. Hood was the one that
19 notified the Secretary of State would be the reason
20 that Mr. Rainer replied to him specifically.

21 Q. Yeah, I don't -- I mean, looking at the
22 email thread again, Mr. Oliver, I don't see where
23 Mr. Hood flags it. It starts with an email between
24 Mr. Rainer and Mr. Koonce, another email between
25 Mr. Rainer and Mr. Koonce, another email between

1 Mr. Rainer and Mr. Koonce, and then Mr. Rainer flags
2 it for Josh Hood.

3 You just don't -- you're just not aware
4 one way or the other why Mr. Rainer sent this to
5 Mr. Hood?

6 A. I'm not -- I'm not aware. I do remember
7 this incident happening, but I don't remember the
8 specifics as to the steps or -- or the procedures
9 and why they were happening.

10 Q. And you don't recall any resolution; is
11 that right?

12 A. No, I don't recall the resolution. No, I
13 don't.

14 Q. All right. Let's look at Exhibit 11.

15 (Plaintiffs' Exhibit 11 was marked for
16 identification.)

17 BY MR. CROSS:

18 Q. All right. Do you see Exhibit 11 in front
19 of you, Mr. Oliver?

20 A. No, I don't. It look like -- my screen
21 disappeared. Give me a second here.

22 Okay. I see it.

23 Q. Okay. And it's just one page. It's a
24 single email.

25 And do you see that this is an email that

1 you sent internally at the Secretary's office on
2 April 24 of 2019?

3 A. Yes.

4 Q. And the subject line that you wrote was
5 "Vulnerability Prioritization."

6 Do you see that?

7 A. Yes.

8 Q. And then you address it to
9 "Infrastructure."

10 Is that how you refer to people here,
11 because they had responsibility for the IT
12 infrastructure?

13 A. Yes. Basically, that would be pretty much
14 the network team, yes.

15 Q. And then you wrote "Please visit the
16 location below to access the spread sheet of the
17 prioritized vulnerabilities (Atlanta Servers) which
18 list the most vulnerable vulnerabilities based on
19 predictive prioritization order. These
20 vulnerabilities are listed in order of priority,
21 please provide mitigation action or feedback."

22 Do you see that?

23 A. I see that, yes.

24 Q. Then there's a link to -- looks like a
25 folder on an H drive at the Secretary's office;

1 right?

2 A. That's correct.

3 Q. What was the purpose of this
4 prioritization of vulnerabilities that you
5 distributed to the infrastructure team?

6 A. The purpose of it was to give them a guide
7 as to which -- what was -- what was labeled as
8 vulnerabilities that needed to -- to be mitigated
9 first. And that could be anything from a critical
10 patch from Microsoft or any other of the vendors
11 that we may have had their hardware or software
12 in -- in our network.

13 Q. What efforts were undertaken at the
14 Secretary's office to identify these
15 vulnerabilities?

16 A. We had several tools that we were running
17 to identify that -- those vulnerabilities, the --
18 the regular -- the regular Microsoft scans; if a
19 system wasn't Microsoft, the scans by that
20 particular vendor.

21 We also had -- ran independent scans based
22 on the procedure that was set up to run scans at --
23 at a particular interval, just to ensure that the
24 state of the system had not changed since the last
25 time a particular scan was ran. So we ran -- we ran

1 scans at certain intervals.

2 Q. So was this a regular process reflected in
3 this email?

4 A. That was a regular process, yes. That --
5 that happened on a -- a regular interval.

6 Q. And what interval was that?

7 A. Typically, it was ran, like, on a weekly
8 basis. This report was sent on a weekly basis.

9 You know, scans -- scans run every day,
10 but the report was -- only ran on a weekly basis.
11 And, basically, it was just to alert the
12 infrastructure staff if they needed to shift any
13 particular priority that they may have been working
14 to mitigate.

15 Q. And when you write to the infrastructure
16 team "Please provide mitigation action or feedback,"
17 was your expectation that the members of this team
18 would provide for you the steps that they were
19 proposing to mitigate these vulnerabilities?

20 A. Yes.

21 MS. LaROSS: Objection to form.

22 BY MR. CROSS:

23 Q. So when you refer to the "prioritization
24 order," how were -- how was the prioritization of
25 these vulnerabilities determined?

1 A. The prioritization was determined by a
2 score that was provided by the various tools that we
3 were utilizing or by a -- by the -- the software --
4 the software put a rating to it, and based on that
5 rating, that's how the priority was assigned.

6 Q. And the mitigation action or feedback you
7 were requesting, did that typically come to you in
8 email?

9 A. It could come in various forms. It could
10 come in an email or it could -- there is a -- a form
11 that they could complete on the -- on the -- on the
12 network.

13 Something like -- something -- as an
14 example, like we had -- we had a tool called Jira,
15 which was like a collaboration tool. They could go
16 into the collaboration tool and put whatever actions
17 or processes that had been taken to mitigate or, if
18 it couldn't be mitigated, as to what the reason it
19 was why it couldn't be mitigated.

20 Q. And can you spell the name of that tool?

21 A. Jira, J-I-R-A, if I'm not mistaken.

22 Q. What's the reference to "Atlanta servers"
23 in parentheses next to "prioritized
24 vulnerabilities"?

25 A. We had a data center in the -- there was a

1 data center in the Atlanta location, and that's what
2 that was referencing.

3 Q. Why did you specifically call out that
4 data center next to "prioritized vulnerabilities"?

5 A. Well, we had -- we had several data
6 centers, and -- and that was just to give them a
7 specific location as to where I was -- what servers
8 I was referring to.

9 Q. Did the Atlanta servers there encompass
10 any components of the election system at this time?

11 MS. LaROSS: Objection.

12 THE WITNESS: In 2019, I would say yes.

13 BY MR. CROSS:

14 Q. Do you recall what sort of vulnerabilities
15 that came up in these weekly reports?

16 A. Not specifically, no. Because like I
17 said, I mean, we get everything from just the
18 regular Microsoft vulnerabilities to Adobe. I mean,
19 anything that -- anything that needed to be patched
20 or updated, to include the operating system. I
21 mean, it could -- it -- once you ran a scan, it
22 identified all of those particular portions of a
23 particular system and it would give you a -- a
24 individual report for every system that you had on
25 your network that you scanned.

1 Q. Why did you and others on the
2 infrastructure team go through this process each
3 week of identifying vulnerabilities?

4 A. Well, that's -- that's just a standard --
5 from a security standpoint, that's just a standard
6 process, is that you continually monitor your
7 systems for vulnerabilities.

8 Just because a system is up to standard
9 today and doesn't have any vulnerabilities on it
10 doesn't mean that this time -- the same time next
11 week, that something is outdated or there has not
12 been an updated patch pushed out by the vendor.

13 So it was a process that -- which you
14 attempted to stay current or as current as possible
15 with your updates and security settings.

16 Q. Why spend time looking for vulnerabilities
17 rather than just looking for actual breaches or
18 actual hacks or comprises?

19 A. Well, vulnerabilities can allow -- if
20 not -- if not mitigated, can open the door or -- or
21 allow a weakness for a -- a hack.

22 As an example, if you -- when you -- when
23 you getting ready to -- when you getting ready to
24 travel -- and this is just an analogy -- but like if
25 you're getting ready to travel, you and your family,

1 you would -- you would do a survey of your home to
2 make sure that all of the windows were secured, all
3 of the doors were secured, there was no items left
4 on your patio or deck that could be used to
5 vandalize or break into your property. So,
6 basically, you're just doing like a walk-through of
7 the area to ensure that there's no known issues that
8 are left that can become a issue while you're away.

9 And the last thing you do is turn -- turn
10 on your alarm system, which is basically what this
11 scan is doing. It's just -- you turn on the alarm
12 system, and it's kind of like detecting if there's
13 any windows or doors open and it allows you to take
14 any actions. If it -- if it comes back and say that
15 the front door is open, then you know that your
16 system -- you can't set your alarm until you go
17 secure the front door.

18 Did that -- did that make sense? I
19 mean...

20 Q. Yes. Thank you, Mr. Oliver.

21 A. Sure.

22 Q. On the software ratings, can you explain
23 how that works? Like, are there certain --
24 presumably there's some sort of assumptions built
25 behind -- built into the ratings in terms of

1 determining what's a high priority and what's a low
2 priority; is that right?

3 A. That is correct, yes. And, basically,
4 that is provided by the -- the IT -- the global IT
5 world. And as an example, I'll just say MS-ISAC is
6 one of the agencies that provide some of these
7 ratings.

8 If a -- if a particular issue has been
9 known to cause issues for various organizations,
10 then it may get a higher rating than an issue that
11 doesn't get any kind of rating or -- or that doesn't
12 affect any -- any company in a major way.

13 Q. The software that you relied on for the
14 prioritization, was that prioritization process
15 tailored specifically to the Georgia Secretary of
16 State's office or was it relying on some sort of
17 standard risk assumptions?

18 A. It is lined -- it is aligned with the
19 standards. And, basically, unless there's something
20 change, what you're -- what you're -- what you're
21 looking to protect is the -- the framework of the --
22 of the system. Because all of -- to include the
23 election system, from what I understand, they all
24 ride on a particular framework. So what you want to
25 do is to ensure that that particular framework is as

1 secure as possible.

2 Q. All right. Mr. Oliver, let's take a look
3 at Exhibit 12.

4 (Plaintiffs' Exhibit 12 was marked for
5 identification.)

6 THE WITNESS: Okay.

7 BY MR. CROSS:

8 Q. All right. Do you see that this is an
9 email that Clark Rainer sent on April 9 of 2019?

10 A. Yes.

11 Q. And you see you're one of the recipients
12 in the "cc" line?

13 A. Yes.

14 Q. I'll come down to the start of it.

15 So it begins with an email from Brendan
16 Marshall at Fortalice Solutions on April 9 of 2019.

17 Do you see that?

18 A. I see that, yes.

19 Q. You see you're one of the recipients of
20 that original email?

21 A. Yes.

22 Q. And the subject line is "Scan Report."

23 Do you see that?

24 A. I see that.

25 Q. And then the email indicates that

1 Mr. Marshall has "uploaded the new scan report to
2 Onehub at this link."

3 Do you see that?

4 A. I see that, yes.

5 Q. It goes on to say "As discussed on the
6 call, it will be most effective to track
7 vulnerabilities by hosts."

8 Do you see that?

9 A. I see that, yes.

10 Q. What's this scan report that's referenced
11 here by Mr. Marshall at Fortalice?

12 A. Basically, Fortalice had the ability, as
13 part of their services, to run scans on -- on -- on
14 our network, whether it be the entire network or
15 just various segments of the network, and we'd
16 typically discuss those on a -- on a routine
17 schedule. Normally -- normally we had a weekly
18 call, but depending on the criticality of what --
19 what may have been in a report as to whether or not
20 we needed to do -- do it any more frequently than
21 that.

22 Q. What is Onehub?

23 A. Onehub was, basically, a -- a secure
24 portal to -- kind of like Dropbox. I mean,
25 that's -- it's not -- I mean, it's not open to the

1 public, but just to give you an example as to what
2 it's like, it's like a -- it's like a secure data
3 storage area.

4 Q. So were these periodic reports or regular
5 reports that Fortalice Solutions did for the
6 Secretary's office on tracking -- tracking
7 vulnerabilities?

8 A. I'm sorry. Say the -- repeat the
9 question.

10 Q. Oh, yeah. Sorry.

11 The scan report that Mr. Marshall
12 mentions, was this a regular report that Fortalice
13 did to track vulnerabilities for the Secretary's
14 office?

15 A. Depending on their engagement. I mean,
16 the answer is yes, at the time that this was being
17 done, yeah, they had a -- they had a -- they had a
18 project where they would engage and scan the network
19 periodically for vulnerabilities, in -- in addition
20 to what we were already doing.

21 Q. Okay. So do you see here the
22 second-to-last email is from Roy Iversen at
23 Fortalice Solutions on April 9, 2019?

24 A. Yes, I see that. Okay.

25 Q. And Mr. Iversen writes "Looking at the

1 results with Brendan - per PCC almost all" -- and
2 "all" is italicized -- "the servers that we have
3 access to scan (and thus in the report) are public
4 facing one way or another, so it is not feasible to
5 triage that way. I have asked Brendan to hold off
6 on sending you yet another spreadsheet, because I
7 don't think it would add more information."

8 It goes on. "In terms of looking at the
9 vulnerabilities here are some thoughts on how to
10 best triage and make progress."

11 Do you see that?

12 A. I see that, yes.

13 Q. When he writes that almost all the servers
14 that they have access to scan are public facing,
15 "public facing" means that they have some sort of
16 connection to the Internet; is that right?

17 A. Yes.

18 Q. Okay. And then "PCC," what does that
19 refer to?

20 A. It's a -- a sub -- a suboffice of a vendor
21 that was in -- in contract with the Secretary of
22 State to provide services.

23 Q. And did PCC's services include a voter
24 registration database?

25 A. I'm not sure. I don't remember.

1 Q. Okay. Where Mr. Iversen provides thoughts
2 on how to best triage and make progress with the
3 vulnerabilities, in the first sentence of the first
4 bullet, he writes "The JBoss and Tomcat
5 vulnerabilities are by far the most critical."

6 Do you see that?

7 A. I see that, yes.

8 Q. What are those?

9 A. They are vulnerabilities identified by the
10 cybersecurity world. They're basically just the
11 name of a -- name of a -- the name of a
12 vulnerability.

13 Like you've heard of -- and this is
14 just -- this is just an example -- like the -- the
15 WannaCry virus. This is just a name that was given
16 a particular vulnerability.

17 Q. Do you recall what the specifics of those
18 vulnerabilities were?

19 A. Not off the top of my head, no.

20 Q. Okay. And then he indicates in the last
21 sentence of that first bullet, "Relying on
22 Cloudflare is just a band-aid that will not prevent
23 a skilled attacker from getting in."

24 Do you see that?

25 A. I see that, yes.

1 Q. Cloudflare was a service that the
2 Secretary of State's office relied on; right?

3 MS. LaROSS: Objection.

4 THE WITNESS: It was one of the services,
5 yeah.

6 BY MR. CROSS:

7 Q. Do you recall whether the JBoss and Tomcat
8 vulnerabilities were remedied as suggested here?

9 A. Yes, they were -- they were remedied.

10 Q. And what measures were taken to remedy
11 those vulnerabilities?

12 A. To the best of my recollection, we ran
13 several updates that mitigated those -- those
14 vulnerabilities.

15 Q. So you didn't simply rely on Cloudflare;
16 is that fair?

17 A. That is correct. I mean, there were --
18 they -- we had a layered -- a layered -- a layered
19 solution, meaning that there was no one product that
20 provided everything inclusively. So Cloudflare was
21 just a -- one layer that we had.

22 Q. Okay. And then Mr. Iversen indicates that
23 "second in importance I would focus on all the
24 Windows patches and .NET patches."

25 Do you see that?

1 A. I see that, yes.

2 Q. In your experience and training in
3 cybersecurity, why are Windows patches important for
4 cybersecurity?

5 A. Well, for one, Windows patches are known
6 worldwide. So if there's a vulnerability in the
7 Windows operating system that's not patched, it
8 means a potential vulnerability for that particular
9 system.

10 Q. So it's important to implement the Windows
11 patches to remedy those vulnerabilities; is that --
12 do I understand that right?

13 A. That is correct, yes.

14 Q. Do you know whether the Windows patches
15 that were recommended here by Fortalice were
16 implemented?

17 A. I would -- I would say yes. Basically, we
18 had a -- we had -- there was a -- there was a -- a
19 schedule to patch system. There was a patch
20 schedule. So systems were patched on a routine
21 basis.

22 Q. And you're talking about the systems that
23 you had responsibility for; right?

24 MS. LaROSS: Objection.

25 THE WITNESS: That is correct.

1 BY MR. CROSS:

2 Q. Okay. Then it goes on. "After that most
3 of the Java vulnerabilities are concentrated on
4 servers where the old version has not been removed."

5 Do you see that?

6 A. I see that.

7 Q. It goes on in the third sentence. "The
8 simple solution is to just uninstall the old
9 version. If Java is no longer required on a server,
10 remove it completely."

11 Do you see that?

12 A. I see that, yes.

13 Q. What measures, if any, were taken with
14 respect to the Java vulnerabilities here?

15 A. Java -- Java was updated. And, again,
16 the -- the patch -- the patch process is a living --
17 is -- is a living process, so it changes day to day,
18 week to week, month to month. And Java -- Java --
19 Java was part of the routine patches that we
20 implemented.

21 Q. Okay. So then back to the most recent
22 email from Mr. Rainer in response to Mr. Iversen's
23 suggestions, Mr. Rainer writes "This is helpful, and
24 as I mentioned earlier I will be talking with PCC
25 tomorrow to escalate the progress of getting these

1 items addressed more aggressively than their typical
2 cycles."

3 Do you see that?

4 A. Uh-huh.

5 Q. Is that a "yes"?

6 A. That is a yes, yes. And --

7 Q. I was just going to ask, Mr. Oliver --

8 A. Go ahead.

9 Q. -- why was there a need for PCC to
10 escalate the progress of getting these items
11 addressed more aggressively than their typical
12 cycles at this time?

13 A. Well, and I'm -- again, it's been a --
14 it's been awhile since I actually looked at the
15 diagram for the network, but PCC was separate from
16 the Secretary of State itself. It provided services
17 to the Secretary of State, but it was not -- it was
18 not physically on the Secretary of State -- in the
19 Secretary of State itself, if I'm -- if I'm -- if
20 I'm -- if you understand what I'm saying. It was --
21 it was a -- it was a different location.

22 Q. Yes, I understand that.

23 What I'm trying to understand is
24 Mr. Rainer indicates that there's some sort of
25 typical cycle that PCC has for addressing

1 vulnerabilities like this.

2 A. Uh-huh.

3 Q. He's going to ask them to escalate the
4 progress of getting these items addressed more
5 aggressively than the typical cycle.

6 What was it about these vulnerabilities
7 that required them to be addressed more aggressively
8 than in the typical cycle?

9 A. I don't -- I don't know at this point. I
10 mean, it could have came in with the higher rating
11 or an urgent rating, which would have probably made
12 Mr. Rainer opt to reach out to them in a more
13 expedient manner because the -- the -- that
14 particular vulnerability may have had a urgent
15 rating.

16 Q. Was PCC slow at addressing vulnerabilities
17 at times? Was that part of the concern?

18 A. At times.

19 Q. Okay.

20 VIDEOGRAPHER: I apologize for the
21 interruption, Counsel. This is the
22 videographer. We're nearing two hours since
23 our last break and I need to take a break to
24 change media units if you don't mind.

25 MR. CROSS: Okay. Let's do that. It's a

1 good time.

2 VIDEOGRAPHER: The time is 11:25 a.m.

3 We're off the record.

4 (Off the record.)

5 VIDEOGRAPHER: The time is 11:45. We're
6 back on the record.

7 BY MR. CROSS:

8 Q. Mr. Oliver, are you familiar with a
9 professor at the University of Michigan named Alex
10 Halderman?

11 A. Alex who?

12 Q. Halderman, H-A-L-D-E-R-M-A-N.

13 A. Not right off my head, no.

14 Q. What is your understanding of what this
15 particular litigation is about that we're here for
16 today?

17 A. Actually, I don't really have a clear -- a
18 clear understanding. The only -- my understanding
19 is that there's -- there's a certain group of
20 individuals that levied a lawsuit against the
21 Secretary of State and the State of Georgia in
22 reference to the legitimacy of voting machines.
23 That's what I kind of understand.

24 Q. Do you understand that my firm and
25 Mr. Knapp's firm represent three voters -- Georgia

1 voters that have brought constitutional challenges,
2 claims that allege that the voting machines that are
3 used in Georgia are not constitutional because they
4 are too unreliable to guarantee the right to vote?

5 Do you understand that?

6 A. I -- I understand the statement, yes, but
7 I was not aware that that's how the lawsuit had
8 instituted, no.

9 Q. And are you aware that in this same
10 litigation, the judge actually entered an injunction
11 in 2019, August of 2019, preventing the State from
12 using the old DRE system?

13 A. That, I am aware of. I had received --
14 I -- I saw that -- I saw that in public forum. I
15 was -- I didn't have any, like, official information
16 on that, but based on public forum, I knew that the
17 judge had made that ruling, yes.

18 Q. And were you aware that that ruling was
19 based, in part, on testimony from our expert,
20 Dr. Alex Halderman?

21 A. No, I was not aware of that, no.

22 Q. Are you aware that Dr. Halderman has
23 analyzed the voting equipment that's used in Georgia
24 today, specifically the BMD, the scanner, the
25 printer that's used, to assess the reliability and

1 security of that equipment?

2 A. No, I was not.

3 MS. LaROSS: Object to form.

4 Go ahead, Mr. Oliver.

5 THE WITNESS: I think I -- I think I
6 got -- I think I answered it already.

7 BY MR. CROSS:

8 Q. So you weren't aware that he issued a
9 detailed report finding that the current system
10 suffers from many significant vulnerabilities?
11 That's not something you heard before?

12 A. No.

13 MS. LaROSS: [Inaudible.]

14 COURT REPORTER: I'm sorry. I can't hear
15 the objections. You're cutting out.

16 Ms. LaRoss, did you have an objection? I'm
17 sorry, Ms. LaRoss, I did not hear your
18 objection.

19 MS. LaROSS: Sure. Objection as to form.
20 Thank you.

21 BY MR. CROSS:

22 Q. Do you understand that the current BMD
23 system uses QR codes to tally votes?

24 A. The answer to that would be yes, but only
25 because I'm a voter in the state of Georgia.

1 Q. Did you -- are you aware that the current
2 election equipment can be hacked in a way that QR
3 codes can be changed so that they don't reflect what
4 the voter actually intended when they voted on the
5 BMD?

6 MS. LaROSS: Objection as to form of the
7 question.

8 THE WITNESS: No, I -- I -- I was not
9 aware that that particular vulnerability
10 existed.

11 BY MR. CROSS:

12 Q. As the former security manager for the
13 Secretary of State's office, if you were still in
14 that role today and had responsibility for the
15 voting equipment, would you take measures to
16 eliminate that vulnerability?

17 MS. LaROSS: I object as to form of the
18 question.

19 THE WITNESS: And ask that question for me
20 again. I'm trying to formulate the answer
21 here. Could you -- could you repeat that for
22 me?

23 BY MR. CROSS:

24 Q. Yeah.

25 If you were -- if you were still with the

1 Secretary's office today as the security manager and
2 had responsibility for the election systems,
3 including the voting equipment, and you learned that
4 QR codes could be changed so that they did not
5 capture the selections voters intended when they
6 voted on the BMD, would you take measures to
7 eliminate that vulnerability?

8 MS. LaROSS: I object to the form of the
9 question.

10 THE WITNESS: And my answer would be kind
11 of in two parts.

12 Having the responsibility would be one
13 thing. Having the authority to actual --
14 actually take actions to mitigate such a
15 vulnerability is another thing.

16 Given the fact -- given that you had both
17 the responsibility and the authority to -- to
18 do so, then my answer would be, yes, I would
19 recommend. Because as the security manager,
20 you can -- you -- your job is to recommend;
21 it's up to the owners of the data to take any
22 kind of mitigation action. But would I
23 recommend various -- investigate and recommend
24 any solutions if there were any? Yes.
25

1 BY MR. CROSS:

2 Q. Are you aware that there are
3 vulnerabilities with the BMD system in Georgia that
4 would allow a hacker to change the human-readable
5 portion of the ballot so that that also did not
6 reflect the actual selections the voter intended?

7 MS. LaROSS: Object to the form of the
8 question.

9 THE WITNESS: Again, I am -- I am aware
10 based on public knowledge. I am not aware from
11 any official capacity that I have served in.

12 BY MR. CROSS:

13 Q. And based on your experience and training
14 in cybersecurity and as the former security manager
15 at the Secretary's office, would it be best
16 practices for the State to remedy that vulnerability
17 as well?

18 MS. LaROSS: Object to the form of the
19 question.

20 THE WITNESS: If it -- if -- if feasible,
21 yes, I would -- I would recommend that that --
22 that be remedied if -- if at all possible.

23 Again, that's without knowing all of the
24 circumstances surrounding such a vulnerability.
25

1 BY MR. CROSS:

2 Q. Are you aware that there are
3 vulnerabilities with Georgia's BMD system that would
4 allow attackers to forge or manipulate the smart
5 cards that poll workers, technicians, use with the
6 equipment during elections?

7 MS. LaROSS: Object to the form of the
8 question.

9 THE WITNESS: The answer would be no.

10 As -- in my role, in the authority that I had,
11 I didn't -- I didn't interact with the election
12 software staff systems in any -- in any kind of
13 major capacity.

14 BY MR. CROSS:

15 Q. If that vulnerability -- if you were aware
16 that that vulnerability existed, based on your
17 experience and training in cybersecurity and as the
18 former security manager for the Secretary's office,
19 would you expect steps to be taken to remedy that
20 vulnerability as well?

21 MS. LaROSS: I object to the form of the
22 question.

23 THE WITNESS: Based on the scenario that
24 you depicted, yes, I would recommend that they
25 look at a solution to -- to remedy such a

1 vulnerability, yes.

2 BY MR. CROSS:

3 Q. Would it surprise you to learn that the
4 Secretary of State's office has taken no measures to
5 mitigate, much less eliminate, any of the
6 vulnerabilities Dr. Halderman has found with the
7 existing system?

8 MS. LaROSS: Object to the form of the
9 question.

10 THE WITNESS: No.

11 BY MR. CROSS:

12 Q. Why not?

13 MS. LaROSS: Again, I object to the form
14 of the question to the extent it relies on the
15 predicate question.

16 THE WITNESS: I guess why not would be
17 kind of -- I would -- I would base it -- I
18 would -- the answer would be based on -- based
19 on my -- my experience as security manager in
20 the role at the Secretary of State.

21 BY MR. CROSS:

22 Q. Can you explain that?

23 A. Well, it would be -- not -- not all
24 recommendations -- not all recommendations were
25 accepted.

1 Q. Cybersecurity recommendations, you mean?

2 A. Right, right. Correct.

3 MR. CROSS: All right. I tell you what.
4 Let's -- I'm getting close to finished. Let's
5 jump off the record just for a few minutes and
6 let me confer with my team, if that's okay,
7 Mr. Oliver.

8 THE WITNESS: Sure, that's fine with me.

9 MR. CROSS: Okay.

10 VIDEOGRAPHER: The time is 11:58. We're
11 off the record.

12 (Off the record.)

13 VIDEOGRAPHER: The time is 12:01. We're
14 back on the record.

15 MR. CROSS: Mr. Oliver, thank you for your
16 time today. I don't have any further
17 questions. I know it was an imposition on the
18 holiday and we feel really bad about that, but,
19 unfortunately, we just couldn't find another
20 time to do this, after having sought to do it
21 over the last several months.

22 So I appreciate you doing it, and
23 hopefully we got you out of here in time to
24 enjoy the rest of the holiday.

25 THE WITNESS: Sure. Thank you.

1 MR. CROSS: That's all we've got. Thank
2 you so much, Mr. Oliver.

3 COURT REPORTER: Ms. LaRoss, you were
4 muted.

5 VIDEOGRAPHER: This concludes --

6 COURT REPORTER: Wait a minute, Jonathan.

7 You were muted, Ms. LaRoss. I didn't hear
8 anything you said.

9 MS. LaROSS: I was just thanking
10 Mr. Oliver. I've got to hit the unmute button.
11 I'm sorry about that. In this day and age
12 where -- I've got it on too much or too little.
13 Anyway, but I was just thanking Mr. Oliver for
14 his time. We very much appreciate it.

15 We also will read and sign, Lee Ann, and
16 would like a rough transcript when it's ready.

17 VIDEOGRAPHER: This concludes the
18 videotaped deposition. The time is 12:02 p.m.
19 Eastern. We're off the record.

20 (Deposition concluded at 12:02 p.m.)


21 (Pursuant to Rule 30(e) of the Federal
22 Rules of Civil Procedure and/or O.C.G.A.
23 9-11-30(e), signature of the witness has been
24 reserved.)
25

C E R T I F I C A T E

STATE OF GEORGIA:

COUNTY OF FULTON:

I hereby certify that the foregoing transcript was taken down, as stated in the caption, and the questions and answers thereto were reduced to typewriting under my direction; that the foregoing pages represent a true, complete, and correct transcript of the evidence given upon said hearing, and I further certify that I am not of kin or counsel to the parties in the case; am not in the regular employ of counsel for any of said parties; nor am I in anywise interested in the result of said case.




LEE ANN BARNES, CCR B-1852, RPR, CRR, CRC

COURT REPORTER DISCLOSURE

Pursuant to Article 10.B. of the Rules and Regulations of the Board of Court Reporting of the Judicial Council of Georgia which states: "Each court reporter shall tender a disclosure form at the time of the taking of the deposition stating the arrangements made for the reporting services of the certified court reporter, by the certified court reporter, the court reporter's employer, or the referral source for the deposition, with any party to the litigation, counsel to the parties or other entity. Such form shall be attached to the deposition transcript," I make the following disclosure:

I am a Georgia Certified Court Reporter. I am here as a representative of Veritext Legal Solutions. Veritext Legal Solutions was contacted to provide court reporting services for the deposition. Veritext Legal Solutions will not be taking this deposition under any contract that is prohibited by O.C.G.A. 9-11-28 (c).

Veritext Legal Solutions has no contract/agreement to provide reporting services with any party to the case, any counsel in the case, or any reporter or reporting agency from whom a referral might have been made to cover this deposition. Veritext Legal Solutions will charge its usual and customary rates to all parties in the case, and a financial discount will not be given to any party to this litigation.



LEE ANN BARNES, CCR B-1852B, RPR, CRR, CRC

1 Diane LaRoss, Esquire

2 dlaross@taylorenghish.com

3 January 24, 2022

4 RE: Curling, Donna v. Raffensperger, Brad

5 1/17/2022, James Oliver (#5036132)

6 The above-referenced transcript is available for
7 review.

8 Within the applicable timeframe, the witness should
9 read the testimony to verify its accuracy. If there are
10 any changes, the witness should note those with the
11 reason, on the attached Errata Sheet.

12 The witness should sign the Acknowledgment of
13 Deponent and Errata and return to the deposing attorney.
14 Copies should be sent to all counsel, and to Veritext at
15 cs-midatlantic@veritext.com

16
17 Return completed errata within 30 days from
18 receipt of testimony.

19 If the witness fails to do so within the time
20 allotted, the transcript may be used as if signed.

21
22 Yours,

23 Veritext Legal Solutions
24
25

1 Curling, Donna v. Raffensperger, Brad

2 James Oliver (#5036132)

3 E R R A T A S H E E T

4 PAGE_____ LINE_____ CHANGE_____

5 _____

6 REASON_____

7 PAGE_____ LINE_____ CHANGE_____

8 _____

9 REASON_____

10 PAGE_____ LINE_____ CHANGE_____

11 _____

12 REASON_____

13 PAGE_____ LINE_____ CHANGE_____

14 _____

15 REASON_____

16 PAGE_____ LINE_____ CHANGE_____

17 _____

18 REASON_____

19 PAGE_____ LINE_____ CHANGE_____

20 _____

21 REASON_____

22 _____

23 _____

24 James Oliver

Date

25

1 Curling, Donna v. Raffensperger, Brad

2 James Oliver (#5036132)

3 ACKNOWLEDGEMENT OF DEPONENT

4 I, James Oliver, do hereby declare that I
5 have read the foregoing transcript, I have made any
6 corrections, additions, or changes I deemed necessary as
7 noted above to be appended hereto, and that the same is
8 a true, correct and complete transcript of the testimony
9 given by me.

10
11 _____
12 James Oliver

_____ Date

13 *If notary is required

14 SUBSCRIBED AND SWORN TO BEFORE ME THIS

15 _____ DAY OF _____, 20____.

16
17
18 _____
19 NOTARY PUBLIC
20
21
22
23
24
25